



Message from FERMA President, Jo Willaert

The senseless devastating attacks in Brussels last 22 March, coming as they do after those in Paris in November 2015, were not just an attack on Belgium, but an attack on the symbol of Europe. Terrorism is a threat for all of our societies, and union and solidarity in the international community are fundamental. These attacks show how important it is for us to manage these risks to the security of our organisations and society as a whole.

A united Europe, determined not to give up the values of freedom and democracy without fear, religious hatred and racism, is the only answer to this barbarity. We will never accept that these actions undermine the will of all Europeans to live and work together.

I would like to thank the many friends and colleagues who have sent messages of concern and solidarity. I in turn send my condolences to the families and friends of those who have been killed and injured.



FERMA calls on EU to put the risk manager at the centre of cyber security

FERMA earlier this month submitted a detailed response, incorporating the views of member associations, to a consultation by the European Commission on cyber security. It stressed to the Commission that boards of organisations need to understand that cyber risk is not only an IT risk but an enterprise risk, and this is where the risk manager provides expertise and quantification of risk.

FERMA President Jo Willaert says, "Without being an IT specialist, the risk manager provides expert advice to support the board and the CEO. He or she works hand in hand with IT and the operational units. Increasingly, also, the risk manager will play a key role in the quantification of cyber risk including through the use of scenario-based evaluations."

The most pressing cyber security challenges for companies today are to maintain public trust, ensure security of the whole supply chain and set up suitable risk mitigating strategies ensuring the continuity of the business, FERMA has told the Commission.

Continue page 2

Also in this issue...

Letter from Brussels	p. 2
Expert View: the SPICE Initiative at Airbus. Philippe Cotelle, Head of Insurance Risk Management, Airbus Defence and Space	p. 3 - 4
FERMA European Risk and Insurance Survey 2016	p. 5
How our world has changed: FERMA's Jo Willaert and AMRAE's Brigitte Bouquot in dialogue with FERMA	p. 6
European news	p. 7
Knowledge corner	p. 8



According to the submission, many businesses have difficulties reaching a basic level of financial protection against cyber risks, often due to a lack of risk insights and data driven risk mitigation. Obstacles include concerns about confidentiality in reporting breaches, lack of clarity on cross-border cyber liabilities and a need to evaluate exposures and validate mitigation measures across the whole enterprise.

FERMA has called for:

- A global set of rules for cyber risk assessment to clarify the conditions for disclosure of sensitive information to third parties;
- A framework that would create a cross-border cyber liability regime;
- The inclusion of cyber risk governance in EU law and regulations;
- At enterprise level, regular, scenario-based evaluations to quantify and validate cyber risk mitigation strategies, including insurance.

Jo comments, “We think legislation and guidance should promote an integrated approach to assessing cyber threats and embed cyber security into the whole organisation - from the top to operational level.”



Letter from Brussels

As you will have seen, FERMA has been active in discussing cyber risks and cyber security at European level this year. What other European issues should we now expect in the next three months?

Environmental liability

The review of the Environmental Liability Directive (ELD) is likely to return to the forefront of European news. The European Commission is expected to release the long awaited ELD report, which will contain conclusions and policy options about the future of the Directive.

FERMA is concerned about the possible introduction of new, burdensome requirements for the EU organisations. They could include the extension of a strict liability regime for a wider list of activities, the extension of the scope of environmental damage (to air, for example) or EU-wide mandatory financial guarantees.

Following publication, the Commission is likely to propose an Action Plan which will be discussed during a stakeholder conference in June. FERMA will closely monitor ELD policy developments and ensure involvement and input in relevant Commission expert groups, consultations and projects.

FERMA recommends to the Commission to consider the value of insurance as part of the cyber security solution – an area missing from the consultation. As the representative body of risk managers in Europe, FERMA is well positioned to contribute to establishing communication between the insurance market and the public authorities that will support the development of a sound cyber insurance market.

FERMA press release:

<http://www.ferma.eu/blog/2016/03/cyber-security-enterprise-risk-ferma-tells-european-commission/>

Full submission to the European Commission:

<http://www.ferma.eu/app/uploads/2016/03/FINAL-response-to-the-2016-cybersecurity-consultation.pdf>

FERMA President’s speech at a conference on cyber risks at the EU Parliament in February:

<http://www.ferma.eu/blog/2016/03/battling-common-enemy-conference-european-parliament-tackle-cyber-threats/>

Country by country reporting

The Commission is now expected to publish by mid-April a proposal extending country-by-country reporting to a wider scope of organisations. The proposal would require multinational corporations to report publicly information on profits, taxes, subsidiaries and tax rulings in all EU countries in which they operate. The details of the proposal are still unknown, but it is likely to take the form of amendments to the existing Accounting Directive.

FERMA calls on the Commission to find a good balance between the right level of transparency and the inevitable administrative costs that the new rules will impose on companies. In the 2014 FERMA European Risk & Insurance Report, a large group of risk managers expressed concern that country-by-country reporting would affect confidentiality of their organisation’s strategy, impact its business model or risk its global competitiveness. It will be interesting to see the reaction in the 2016 survey when country-by-country reporting is closer to a reality.

FERMA is following the discussions closely and will react to the Commission’s proposal. Joint lobbying activities with other stakeholder are in the pipeline, notably a conference in May with European Confederation of Institutes of Internal Auditing (ECCIA).

Insurance Block Exemption Regulation

The Commission has now released its report with preliminary conclusions about the future of the Insurance Block Exemption Regulation (IBER). FERMA will participate in the stakeholder meeting planned on 26 April and restate our support for the renewal of the IBER for (re)insurance pools.

Typhaine Beaupérin, CEO of FERMA

Cyber risks: the SPICE Initiative at Airbus

Philippe Cotelle, Head of Insurance Risk Management, Airbus Defence and Space



There are three main obstacles to a good understanding of cyber risks in our organisations, which I believe are common to most businesses.

1. It has long been perceived as an IT issue only, which neglects addressing the related business impact. This is especially critical with the increase in connectivity of industrial systems.
2. Confidentiality is a major element preventing a clear and open analysis of this risk as information management is a critical security issue; even creating a list of potential vulnerabilities is a huge concern.
3. Finally there is a fear that disclosing a cyberattack suffered or even admitting a potential vulnerability could endanger the reputation of the company.

To get over these obstacles, the risk manager has to be able to demonstrate to the CEO or the executive committee the possible financial impact of a massive cyber attack in terms of business interruption and loss of business opportunity. For this, the risk manager needs data to show the organisation's current state of cyber resilience, past and future cyber protection investments, and mitigation of the risk.

We must also be able to explain the legal and regulatory implications of dealing with data breaches, especially under US laws, and the protection of critical infrastructures under French and EU laws.

The risk manager needs a cyber risk map of the information system of the organisation showing the most sensitive assets to be protected. Finally he or she will use this information to engage with the insurance market.

No convincing method available

We found that no convincing method had already been developed for doing this; we had to elaborate one. SPICE stands for **s**cenario **p**lanning to **i**dentify **c**yber **e**xposure, and it is an initiative sponsored by the CFO of Airbus Defence and Space, initiated by me as the Head of Insurance Risk management.

It is a pilot programme for a business impact analysis to identify cyber-related disaster scenarios that could affect our operational capability and it is truly innovative.

SPICE needs high level technical experts who know the cyber threat environment of the organisation. To start, we gathered representatives of all the functions as well as from IT and information management security to:

- Educate the operational managers to the new cyber threats;
- Discuss the security issues with great care;
- Openly consider some potential cyber attack scenarios – and not assume it could not happen to us;
- Support 'impacted' functions and information management security.

Building the scenario

Attacks: We focussed on identifying potentially catastrophic scenarios:

- Who might attack us and what would their motives be?
- What functions and assets would be impacted?
- How would we recover and how long would it take?

Cost: We calculated the business and operational impact with inputs from operations.

We split the scenarios into four phases from security breach to recovery, including investment in remediation, to estimate the possible costs at each phase. What did we learn from this?

- The numbers relate to our financial exposure – but there is no final number.
- Management has to play a part.
- The objective is to reach a consensus that is acceptable to everyone and valid for our analysis.

Probability: Local information management security then evaluated the technical probability of the success of an occurrence at each step of the process. For this we used the Cyber Kill Chain developed by Lockheed Martin, which plots the stages of an attack from preparation, instruction and active breach against the time involved.

Lessons: This same method applied by experts at two different sites produced two different probability numbers. We learned that we need a homogenous approach, but that it also has to be associated with different types of attackers, from malicious individuals, to organised criminals or foreign government agencies. We have to ask – why would they undertake the specific attack which is the subject of our scenario?



Mitigation: SPICE helps us develop our mitigation security plan and link it to business needs. We measured the costs of implementing further IT security measures to reduce the probability of occurrence and as a consequence the resulting exposure. After making this IT investment, it makes economic sense to evaluate how to mitigate the residual exposure through insurance. We have the basis for a dialogue with the insurance market to complement this mitigation strategy with an insurance programme tailored to our needs.

Conclusions:

- We believe this methodology is key in obtaining valuable insight into our cyber risk exposures.
- This process needs to be performed regularly and as exhaustively as possible.
- We have to be able to roll out the process across the whole company, its products and its locations.
- We must be able to work with operations.
- SPICE provides elements for the risk manager to enlarge the current scope of ERM to encompass cyber risks.

When it comes to cyber risks, many challenges remain in front of us. There is simply no one response. At the same time, there is no alternative to the development of the digital economy, and industry has to adapt thanks to the new possibilities offered by technology to improve efficiency, reliability and profitability. This opportunity, however, generates in itself new risks which have to be addressed and for which a dedicated risk management policy has to be defined. We need a collective effort coordinated between industry, the insurance market and the public authorities. It is time to move from awareness to action

Philippe Cotelle, Head of Insurance Risk Management at Airbus Defence and Space is a member of AMRAE and has been supporting FERMA in the development of its response to the European Commission's consultation on cyber risk. He is also working with François Beaume, President of AMRAE's commission on information systems.

For Philippe Cotelle's presentation on SPICE at the FERMA Forum 2015, see :
<http://www.slideshare.net/FermaForum/philippe-cotelles-presentation-on-spice-at-airbus-ferma-forum-2015?sm.tNoRedir=1>.

FERMA European Risk and Insurance Survey 2016 Sponsors

XL Catlin, AIG, Chubb, Marsh, EY



CHUBB

MARSH



FERMA Survey 2016 opens soon! This is about you, risk and insurance manager

Just ahead of the launch of 2016 FERMA European Risk and Insurance Survey on 8 April, FERMA Vice-President and Survey project chairman Cristina Martinez has urged her colleagues to participate.

“We need your input,” says Cristina. “The more responses we receive, the more useful the results are for you in your work and for FERMA in serving you.”

As she explains, “This is an opportunity to contribute to a unique resource for risk and insurance managers. It is now in its eighth edition. This means we can see how we have developed as a profession since the first edition in 2002, and where we are today in a world which has changed dramatically. This is about you, risk and insurance manager.”

The questions for the 2016 survey build on core elements from previous editions and include updates. According to Cristina, “This strengthens our ability to see where we have come from and where we are today. We have also taken into account the feedback we received and have made the questionnaire shorter and simpler.”

The results of the survey will be published in the FERMA European Risk and Insurance Report at the FERMA Seminar in Malta on 3-4 October. It will then form the basis of further research by FERMA and member associations, as well as providing benchmarks for individual risk managers to use in their own work.

Cristina adds that the survey supports the three themes of FERMA President Jo Willaert and of the Seminar: education, communication and leadership. “The results are part of our continuing education and recognition about the profession. They give us solid data to help us to exercise risk leadership.”

For questions about the survey, contact Laëtitia Fung at administration@ferma.eu Laëtita has joined FERMA as Project Officer in charge of the Survey, and she provides organisational and administrative support to the team.

This is about us! Three leading risk managers explain why they complete the survey questionnaire.



Dirk Wegener, Vice-President of FERMA: “By participating in the survey, we strengthen the effectiveness of this tool for our own benefit. Secondly, we have a say in setting the agenda for our profession by highlighting topics which we perceive to be important. The higher the response rate, the more valuable the survey is for us.”



Helle Friberg, FERMA board member: “I always complete the survey because I find the outcome of it quite valuable. It tracks trends over time, including the development of our profession, and it reveals what the current significant concerns are. There is great benchmarking value to gain from the survey. It is important for us to complete the questionnaire so that it reflects the risk and insurance management situation of a broad section of European companies.”



Patrick Smith, President of Airmic: “I always participate in the FERMA survey because it represents the only pan-European collation of risk managers' perspectives on the key issues relating to risk and insurance, and their relevance and maturity within their organisations. The greater the participation the more reliable and interesting the results, so I encourage my risk and insurance manager colleagues to contribute.”



Julien Bedhouche, FERMA

Risk conversation at board level: Data protection

The new EU Data Protection Regulation, which will come into effect in 2018, creates a completely new regulatory regime for organisations holding personal data. It comes with the risk of substantial penalties for breaches.

To discuss the implications of this new Regulation, FERMA co-organised a webinar with AIG and the directors' organisation EcoDA on 23 February: "How to adapt risk governance to the changing regulatory landscape for personal data".

The speakers were Vivian Walry, a partner in CMS DeBacker Luxembourg; Thomas Koch, senior manager at KPMG; and Marie-Gemma Dequae, scientific adviser to FERMA. The moderator was Roger Barker of ecoDA.

Full recording of the session:

<https://attendeegotowebinar.com/recording/5259822107520161027>

Presentations: <http://www.ferma.eu/blog/2016/02/9643/>

They stated that:

- The penalties for breaches can be fines of up to €10m or 2% of global turnover or up to €20m or 4% of global turnover for groups of enterprises.
- Yet, there is evidence that many boards are still not fully aware of how their companies use data or how they will meet the new reporting requirements.
- Data risk management should be part of enterprise risk management (ERM) and reporting should be at high levels.
- Protection for privacy should be embedded in each new product and process by design and by default.
- Because data breaches can still occur, the risk should be included in business continuity and crisis management to mitigate its potential impact.

This was the second in the series of FERMA webinars on the risk conversation at the board level. It is part of FERMA's continuing programme of information on EU issues for its members. The next one took place on 24 March on cybersecurity mitigation strategies. More information in the next FERMA newsletter.

Commission proposes non-renewal of IBER

On 17 March, the European Commission released its report with preliminary conclusions about the future of the Insurance Block Exemption Regulation (IBER). In it, the Commission states that the renewal of the IBER for (re)insurance pools does not appear justified because of its limited use and relevance.

FERMA has argued for the retention of the IBER saying its loss would change radically the coverage of large and exceptional risks, such as terrorism, but not widen choice for commercial insurance buyers.

A stakeholder meeting is planned on 26 April to discuss the options: to renew the regulation in its current form, modify it or let it lapse. FERMA will participate in the event to raise the voice of business customers and users of these (re)insurance pools and continue to advocate an exemption from EU competition rules for the IBER.

The expiry date of the current IBER is 31 March 2017.

More details at:

European Commission press release:

http://europa.eu/rapid/press-release_IP-16-861_en.htm

Report on the functioning and future of IBER:

http://ec.europa.eu/competition/sectors/financial_services/iber_report_en.pdf

FERMA 2014 press release:

<http://www.ferma.eu/blog/2014/11/coverage-largest-exceptional-risks-still-needs-exemption-eu-competition-rules/>

Third Webinar on cybersecurity mitigation strategies took place on 24th March with an average audience of 120 participants

Have a look at the Presentation slides:

<http://bit.ly/1WZFiMd>

