FERMA
Federation of European
Risk Management Associations

Av. Louis Gribaumont 1, B4
1150 Brussels. Belgium
T: +32 (0)2 761 94 32
F: +32 (0)2 771 87 20
E: info@ferma.eu
www.ferma.eu

Response to the European Commission consultation on the public-private partnership on cybersecurity and possible accompanying measures

11 March 2016

Executive Summary

The Federation of European Risk Management Associations (FERMA) welcomes the opportunity to contribute to the Commission consultation on the public-private partnership on cybersecurity and possible accompanying measures that could stimulate the European cybersecurity industry.

FERMA represents the interests of more than 4700 European risk and insurance managers, who are business users of cybersecurity solutions. Because of their fast moving nature, cyber risks are threatening the successful achievement of organisations' objectives. As for any other risk, the risk manager brings a unique added value in identifying and quantifying the cyber risk exposure. This is a necessary step towards understanding and managing the exposure of the company through the use of cybersecurity solutions.

FERMA main points:

- Cybersecurity products and services in Europe are available at very good standards. The main issue is not the lack of cyber products but the lack of education and awareness of the impacts that cyber attacks can have on the business as a whole, which are often underestimated by businesses.
- FERMA regrets the lack of focus on the risk governance aspect of cyber security in EU cybersecurity laws, which is essential to embed cyber security into the organisation, i.e. from the top to operational level. Such good cyber risk governance should be aligned with the internationally agreed three lines of defence model.
- Cyber risk is not only an IT risk; it is an enterprise risk. Cyber security should be integrated into the enterprise risk management (ERM) system of the organisation, with the board playing a critical oversight role and the risk manager providing expert advice to support the decision-making process.
- Scenario-based impact evaluations should be performed on a regular basis to validate the mitigation strategies of organisations and increase the overall resilience of the economy.
- FERMA recommends developing a common framework for cross-border liability related to a cyber event, a global set of rules for cybersecurity risk assessment and a European database of cyber insurance claims.

- FERMA can contribute to the establishment of a dialogue with the insurance market and public authorities that will support the development of a sound cyber insurance market. It is necessary to unlock the cyber insurance market to support the economic growth that the digital world is bringing to Europe.

1. Assessment of cybersecurity risks and threats

1.1. RISK IDENTIFICATION

1.1. What are the most pressing cybersecurity challenges for users (individuals, business, public sector)?

With an even more digital economy by 2020, public trust in using and buying services/products online is a top priority for companies for doing business. It is also a question of reputation. Disclosing a cyber attack or even admitting a potential vulnerability to a cyber attack is endangering the reputation of the company which could raise concerns among their customers, investors and counterparties.

The resilience of the whole supply chain is also a pressing cyber security challenge for businesses. Weaknesses of only one sub-contractor can impact the rest of the supply chain leading to economic losses and even jeopardising the existence of some partners.

Organisations are increasingly facing new cyber risk exposures, both in terms of first party risk exposures and third-party liability exposures, with serious regulatory consequences from the latest cyber laws. The challenge is to protect the organisation's assets by putting in place suitable risk mitigation strategies, so that it continues to prosper and grow in a highly competitive environment.

1.2. PREPAREDNESS

2.1. Are the necessary products/services available on the European market to ensure security of the whole value chain?

FERMA believes that cyber security products and services are available on the European market at very good standards.

The main issue is therefore not the lack of cyber products, but a lack of education and awareness of the impacts that cyber attacks can have on the business as a whole, which are often underestimated by businesses. As a result, budgets allocated to IT security are not in line with the magnitude of the risk.

This said, the offer of cyber products and services will never cover all the risks due to the accelerating pace of innovation. It is the role of insurance to cover these residual risks.

1.3. CYBERSECURITY CHALLENGES BY 2020

4.1. What will be the 3 main cybersecurity challenges by 2020? (Please explain)?

FERMA considers that the main cybersecurity challenge by 2020 is to develop catastrophic cyber loss scenarios for use by organisations as stress tests to validate their mitigation strategies and increase the overall resilience of the economy. This scenarios will allow to:

- Estimate the possible costs for each identified business and operational impact;
- Prioritise investments and optimally aligning computer security defences with the threats that pose the greatest risk to business environments;
- Start a dialogue with the insurance market to complement the mitigation strategy with an insurance programme tailored to the needs of the organisation.

These scenario-based impact evaluations should be performed on a regular basis.[1]

To help organisations coping with this challenge, FERMA believes that a global set of rules for cyber risk assessment (i.e. the quantification of the cyber risk exposure) should be put in place:

a. Internally as a basis for risk managers to address the exposure and develop risk mitigation strategies.
b. Externally for an accurate pricing of the residual risk by the insurance market community.

Furthermore, a common framework for cross-border liability related to a cyber event is essential to allow a clear allocation of the liability among the involved parties and develop recourse actions for the victims.

2. Cybersecurity Market Conditions

6. How does legislation (currently in force or soon to be adopted) influence the European cybersecurity market(s) or how is it likely to do so?

In general, mandatory measures and binding rules are powerful triggers for the adoption and/or purchase of specific products. Legislation is therefore likely to increase the demand for cybersecurity solutions that will fit the requirements of the law.

The regulations then become not just a matter of compliance for the organisations but also a condition for doing business. For instance, in February 2015, the US Securities and Exchange

[1] One relevant illustration of this response methodology is the Airbus pilot programme SPICE (Scenario Planning to Identify Cyber Exposure) for a business impact analysis to identify cyber-related disaster scenarios affecting operational capability. See from slide 41 at http://www.ferma.eu/app/uploads/sites/6/2015/10/2015.10.06-Cyber-Risks.pdf

Commission ("SEC") mentioned proof of cyber insurance as one element that could be required during a cyber breach investigation.[2]

In the EU, the NIS Directive and the Data Protection Regulation will oblige organisations to prepare themselves for the notification of incidents and data breaches to their local supervisors. This includes not only the ability to provide the required documentation such as impact assessments and information security policies to local supervisors, but also the training of legal staff and those who are closely involved in managing reputation (e.g. public relations, media, social media), whose costs can be covered by specific insurance policies.

Regulation and compliance with the potential for sanctions and fines and accompanying reputation risk appear to be driving much of organisations' planning around cyber risk, including the purchase decision of cybersecurity products to prevent and/or mitigate potential damages.

FERMA however regrets the lack of focus on the risk governance aspect of cybersecurity in EU cybersecurity laws. The legislation contains very few elements on corporate governance which is essential to embed cyber security into the organisation – i.e. from the top to operational level. Cyber risk is not only an IT risk, but an enterprise risk. An integrated approach to assessing cyber threats and protecting the organisation's assets is necessary.

Cybersecurity laws are also likely to result in more claims for the emerging cyber insurance industry. The increased use of personal data in connected devices, social media, geotagging, etc. will lead to more data breach possibilities. This, combined with the high sensitivity of civil society to data privacy, will have an impact on claims, although it is still unclear, probably too soon, to see how insurers will price and deal with certain type of threats.

3. Need for public intervention and support for a functioning market in cybersecurity products/services in Europe

3. How do you assess public support and intervention at national level with regard to the cybersecurity market? How useful / necessary / adequate is it? (Please specify)?

Some EU member states have taken interesting initiatives for cybersecurity like the Cyber Essentials in the UK (see response to Q4). FERMA believes that public intervention is necessary particularly in the areas listed below in order to support organisations and especially the risk managers whose role is to identify, quantify, evaluate, mitigate and transfer risks:

- Establish a common framework for liability along the supply chain to the end customers. This common framework would clearly define who carries which risk and in which proportion.

[2] (See page 5) OCIE's 2015 Cybersecurity Examination Initiative. (2015). [online] Available at: https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf [Accessed 10 Mar. 2016].

- Develop a framework for cybersecurity risk assessment, notably including a certification process for compliant organisations and a mandatory disclosure of risk exposure to the public authorities.
- Support the risk transfer process by facilitating the management of cyber insurance claims:
    - Organise intermediation by empowered public officers in order to preserve the confidentiality of the insured party and help the insurer to settle the loss.
    - Organise the disclosure process to the potential third party victims of the claim.
- Create a European database of cyber insurance claims in order to have up-to-date status on cyber threats and the costs of known losses and thus improve the management of cyber risks.

4. Please provide examples of successful support through public policies (at national or international level).

In June 2014, the British government launched a joint initiative with some major British insurers to increase the level of IT security in UK companies. The Cyber Essentials scheme is based on certificates. It ensures that certified organisations have a certain amount of security measures in place.

The following national initiatives should also be noted:

- In Germany, the "Alliance for Cyber Security", founded by the Federal Office for Information Security (BSI) in cooperation with the Federal Association for Information Technology, Telecommunications and New Media (BITKOM). This public-private partnership serves to provide to the German industry participants with up to date knowledge about cyber threats and decrease the response time in case of cyber attacks. The participants can also contribute to increasing the knowledge base by (anonymously) reporting incidents.
- The recent development of French legislation according to the "Loi de Programmation Militaire" and the obligations for organisations qualified as "Opérateur d'Importance Vitale"(similar to CNI- Critical National Infrastructure). The status of Opérateurs d'Importance Vitale (OIV) puts certain private or public organisations of strategic importance under specific rules regarding cyber security. It empowers the French Network and Information Security Agency (ANSSI, Agence Nationale de Sécurité des Systèmes d'Information) with specific control and investigation powers over the OIVs. The overall objective is to preserve the competitiveness of the OIVs by countering the risk of theft of intellectual property and trade secrets.

4. The role of research and innovation in cybersecurity

7. What would be your contribution to fostering innovation and competitiveness of cybersecurity in Europe?

Cyber risk is not only an IT risk; it is an enterprise risk. FERMA therefore advocates a central role for the risk management function as regards cybersecurity in the company.

Cyber risk is today a risk that every company is faced with. Nevertheless, businesses have difficulties with reaching a basic level of protection often due to a lack of risk insights and data driven risk mitigation. Given its strategic importance, cyber security should be integrated into the enterprise risk management (ERM) system of the organisation, and boards should play a critical oversight role. Risk management is a collective tool and part of the internationally agreed three lines of defence model.Therefore the governance of cyber risks should be established in accordance with this model.[3]

The role of the risk manager is crucial to support the decision-making process. Following a risk-based approach, the risk manager aims to build a shared understanding of the company's exposure allowing prioritisation of investments and optimal alignment of computer security defences with the threats that pose the greatest risk to business environments.

The risk manager organises, as for other risks, the quantification aspect of cyber security. This is a necessary step for understanding and managing the exposure of the company. To achieve this, the risk manager works hand in hand with the operational departments (IT, legal, internal audit and others) without being himself or herself an IT specialist. The risk manager is responsible for making proposals to the board for risk mitigation strategies and financing strategies for the residual value at risk.

In companies where risk management is part of the decision-making process, this will naturally lead to global solutions, and stand-alone insurance coverage for cyber security will be one of them. However, the growth of the cyber insurance market is much slower than expected for three main reasons:

1) First, in order to provide insurance coverage with an appropriate premium, the insurers may need underwriting information in connection with the key strategic assets of the organisations. The future insured might have to disclose sensitive information and in some cases allow a pre-underwriting assessment by a third party.
   A common framework on risk analysis should match the need for confidentiality and the expectations from insurance market and public bodies.

[3] Audit and Risk Committees: News from EU Legislation and Best Practices. (2014). [online] FERMA / ECIIA, p.10. Available at: http://www.ferma.eu/blog/2014/12/ferma-eciia-respond-new-corporate-transparency-requirements/ [Accessed 10 Mar. 2016].

Public authorities must play a role to provide guarantees about how the information is treated within the insurance community. Certification programmes for cybersecurity providers may help provide these guarantees.

2) The second issue is reputational and linked to an insurance claim. The notification of such an event would involve a number of different players: the broker, all the insurers on the programme, their reinsurers, loss adjustors, etc. It is a challenge to ensure that critical information remains confidential despite the number of involved parties.
3) The last issue relates to the claim settlement. As cyber is a technical risk, the insurers would require third party experts to evaluate the company's systems and confirm the extent of the loss and the application of the coverage. Are companies ready to let those third parties access the most critical and secret part of their systems?

These issues are the key subjects to unlock the cyber insurance development and support the economic growth that the digital world is bringing to Europe. As the representative body of risk managers in Europe, FERMA can contribute to establishing a dialogue with the insurance market and the public authorities that will support the development of a sound cyber insurance market.

Contact person: Julien Bedhouche, FERMA EU Affairs Adviser, julien.bedhouche@ferma.eu

FERMA - The Federation of European Risk Management Associations brings together 23 national risk management associations in 21 European countries. FERMA represents the interests of over 4700 risk and insurance managers in Europe active in a wide range of business sectors from major industrial and commercial companies to financial institutions and local government bodies. More information can be found at www.ferma.eu