Position Paper

FERMA's comments submitted on the Consultation on the revision of the NIS Directive

2 October 2020

Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the EU (hereafter "the NIS Directive") has been instrumental in building Europe's capacity to withstand cyber-attacks, which helps to foster greater economic resilience. Alongside the General Data Protection Regulation (GDPR), the NIS Directive has greater sensitized European businesses to data and systems security. This is a laudable achievement.

But as this year has shown, the EU must strive to ensure a state-of-the-art response reflecting the needs for increased cybersecurity. The COVID-19 pandemic and its implications on teleworking and digital infrastructure on the whole, as well as the increasing frequency and costs of cyber attacks underline these needs.

This EU-level response should focus on increasing preparedness at national and Union level by building up **robust capabilities to prevent, detect, respond to and mitigate cyber threats in times of crisis**. It should also enable a swift re-start of activities.

In addition, FERMA encourages the European Commission to use this review of the NIS Directive to consider how it can engender a more open culture of exchanging of information on incidents and threats in the EU. The GDPR and NIS Directive have created a raft of data and "intelligence" on threats and incidents but FERMA is concerned that there has not yet been a cultural shift where collaborative exchange of information systematically takes place between all stakeholders. FERMA and its members are very keen to engage further with the European Commission on this point.

With regards to our specific comments on the review of the functioning of the NIS Directive, FERMA calls upon the European Commission to consider the following arguments:

1) place a greater emphasis on the risk management approach to boost resilience
2) expand the scope of the NIS Directive
3) give further consideration to the building up of financial capacity to help shoulder future catastrophic events

The important role of risk management to build a strong culture of cybersecurity within organisations must be underlined. FERMA, together with The European Confederation of Institutes of Internal Auditing (ECIIA), has addressed this very topic in a 2019 joint paper that advocates for cyber risk governance models that go beyond the implementation of IT measures in order to efficiently protect organisations' assets and ensure their resilience and continuity. The model is anchored in two strong sets of principles: the eight principles set out in the OECD recommendation on Digital Security Risk Management (2015) and the Three Lines of Defence model, recognised as a standard of Enterprise Risk Management (ERM).

FERMA believes it is necessary to expand the scope of the NIS Directive with the aim of creating greater harmonisation across the Union. For the risk management community, cyber resilience is about having at least the following three steps in place:

- a risk prevention policy
- a crisis management plan
- a recovery/business continuity plan

The NIS Directive should enhance the cyber resilience of all sectors by increasing the level of harmonisation requirements and thereby reduce fragmentation of the internal market. While FERMA is concerned that sector-specific legislation may leave other sectors more exposed to cyber-attacksm it is also of the view that the proposed regulation [2020/0266 (COD)] on digital operational resilience for the financial sector is a crucial first-step in raising operational resilience in an important sector. However, the financial sector does not exist in isolation.

FERMA is of the view that the NIS Directive could be used to foster a mechanism that responds to and mitigates cyber threats and be prepared to act in crisis, based on a sound foundation of risk management grounded in the Three Lines of Defence model. While the Three Lines of Defence model will assist in increasing preparedness, there are some risks facing organisations that need to be transferred. This is where cyber insurance comes in as a key contributor to the overall goal of increasing cyber resilience. FERMA has advocated for the EU to take concerted efforts to stimulate the capacity of the EU cyber insurance market. Unfortunately, the increased digitalisation of the modern economy also exposes it to greater cyber risks, for which the insurance industry alone does not have the material capacity to cater. It should not therefore be for the insurance industry alone to shoulder this burden and Member States and the European Union should also help to ensure that essential service providers have the appropriate financial protection. **Thus, the NIS Directive should focus towards building material capacity within the insurance and financial sectors to help shoulder future catastrophic events.**

Lastly, and as a broader comment, FERMA calls upon the European Commission to give further consideration to building up financial capacity to help foster resilience in the face of future catastrophic events of all kinds. The very nature of the digital economy (i.e. interconnection) means that risks increasingly look (and are) systemic. Such risks would also be cross-border, and not just European—similar in a sense to the risks emerging from the Coronavirus pandemic. This situation, however, gives the opportunity for European to take the lead on solutions. While some Member States have established pool-type solutions to cover certain types of systemic risks such as terrorist attacks, this is not a uniform approach to the problem. Furthermore, there are no national pool-type solutions that exist that offer protection from a future disruptive event taking the form of a global cyber-attack that will impact millions of devices across multiple industries and critical infrastructures. On this topic, FERMA has proposed an EU Resilience Framework for Catastrophic Risks, which you can read here.

FERMA looks forward to engaging further on this topic with the European Commission.

Contact person: Charles Low, FERMA Head of EU Affairs, Charles.low@ferma.eu

FERMA - The Federation of European Risk Management Associations brings together 22 national risk management associations in 21 European countries. FERMA represents the interests of more than 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