European Commission Contractual Public-Private Partnership on Cybersecurity

Introduction

On the 6th May 2015, the European Commission adopted the Digital Single Market (DSM) Strategy, which provides for establishing a contractual Public-Private Partnership (cPPP) on cybersecurity in the area of technologies and solutions for online network security in the first half of 2016.

The establishment of a cPPP addressing digital security would be a further step towards cybersecurity industrial policy. The Commission is now considering what additional industrial measures may be needed to complement the cPPP.

The cPPP will be a contractual arrangement between the Commission and an industrial grouping, both of which are committed to supporting, in the EU's Horizon 2020 programme, research and innovation activities of strategic importance to the Union's competitiveness in the field of cybersecurity.

A cPPP bringing together industrial and public resources would focus on innovation following a jointly-agreed strategic research and innovation roadmap. It would make the best possible use of available funds through better coordination with member states and a narrower focus on a small number of technical priorities. It should leverage funding from Horizon 2020 to deliver both technological innovation and societal benefits for users of technologies (citizens, SMEs, critical infrastructure), as well as provide visibility to European Research and Innovation excellence in cyber security and digital privacy. Furthermore cybersecurity is explicitly identified in the DSM strategy as a priority area in which there is a need to define missing technological standards.

Background

On the 7th December 2015, after over a year of negotiations, the European Parliament and the EU Council of Ministers reached informal agreement on the Network and Information Security Directive ("NIS Directive").

This landmark Directive – the first time the EU has legislated on cybersecurity – aims to establish a harmonised set of requirements for certain businesses; i.e. essential services operators and digital services providers, to make them cyber-attack proof.

Key points[1]

- **Application** - The NIS Directive imposes obligations on operators of essential services and providers of key digital services and lists the essential services to which it applies. This list

[1] Source: Lloyd's of London

includes, among other sectors, transport, banking, financial market infrastructures, healthcare and energy. It does not, however, mention insurers explicitly.

- **Minimum harmonisation** - The Directive sets out minimum harmonisation measures and Member States are not prevented from adopting more restrictive provisions to achieve higher levels of NIS security. In the implementation phase, it is for Member States to identify specific entities, under each sector listed, to which the rules will apply.
- **Increased national cybersecurity capabilities** - Each EU Member State must adopt a national strategy and appropriate cybersecurity measures. They must establish a National Competent Authority (NCA) to monitor implementation of the rules, as well as Computer Security Incident Response Teams responsible for handling incidents.
- **Security and notification requirements** - The businesses to which the Directive is applied will have to take appropriate security measures to manage the risks posed to the network and information systems they control and use in their operations. They will be required to notify to the relevant NCA, without undue delay, incidents having a significant impact on the continuity of the core services they provide.
- **Cooperation network** - The EU Commission and the NCAs will form a cooperation network tasked with supporting and facilitating strategic cooperation and exchange of information.
- **Sanctions** - Breach of the obligations imposed by the Directive may attract onerous administrative sanctions. It is the responsibility of Member States to determine penalties which, according to the Directive, must be "effective, proportionate and dissuasive".

The Survey

The Commission is consulting stakeholders on the areas of work of the future cybersecurity cPPP. The Commission is also calling for contributions on potential additional policy measures that could stimulate the European cybersecurity industry.

The survey focuses on the technical aspects of cybersecurity; i.e. what should be the main priorities of technological areas of embedded systems, cloud computing and hardware/software engineering. It is less about the end-user, which the AAE can meaningfully contribute to. To put in context, AAE could perhaps, at a stretch, contribute to about 5% of the questions. Additionally, insurers are not specifically mentioned in the list of operators of essential services and providers of key digital services.

Information for the AAE

The borderless and multi-layered Internet has become one of the most powerful instruments for global progress without governmental oversight or regulation. While the private sector should continue to play a leading role in the construction and day-to-day management of the Internet, the need for requirements for transparency, accountability and security is becoming more and more prominent.

Principles of cybersecurity

- The EU's core values apply as much in the digital as in the physical world;

- Protecting fundamental rights, freedom of expression, personal data and privacy - Cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values;
- Access for all - The Internet's integrity and security must be guaranteed to allow safe access for all;
- Democratic and efficient multi-stakeholder governance - The EU reaffirms the importance of all stakeholders in the current Internet governance model and supports this multi-stakeholder governance approach;
- A shared responsibility to ensure security - The growing dependency on information and communications technologies in all domains of human life has led to vulnerabilities which need to be properly defined, thoroughly analysed, remedied or reduced. All parties need to recognise this shared responsibility, take action to protect themselves and if necessary ensure a coordinated response to strengthen cybersecurity.

Five strategic priorities

The EU vision presented in this strategy is articulated in five strategic priorities:

1. Achieving cyber resilience;
2. Drastically reducing cybercrime;
3. Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP);
4. Develop the industrial and technological resources for cybersecurity;
5. Establish a coherent international cyberspace policy for the European Union and promote core EU values.

Impact of cybersecurity on the Insurance market

A UK Government survey estimated that in 2014 81% of large corporations and 60% of small businesses suffered a cyber breach. The average cost of a cyber-security breach is £600k-£1.15m for large businesses and £65k-£115k for SMEs. The existence of cyber insurance is aimed at protecting businesses against risks of business interruption, income loss, damage management and repair, and possibly reputational damage if IT equipment or systems fail or are interrupted.

While existing insurance policies such as commercial property, business interruption or professional indemnity insurance, may provide some elements of cover against cyber risks, businesses are increasingly buying specialised cyber insurance policies to supplement their existing insurance arrangements.

Impact of the NIS Directive and consequently the cPPP on insurers and the insurance market are as follows:

- Risk management implications - Although insurers are out of the scope of the Directive, the final decision on whether certain entities meet the Directive’s criteria will be remitted to Member States.
- Impact on underwriting - Once the NIS directive is implemented, it may drive demand for cyber insurance in Europe.

- The new EU rules support the creation of a risk management culture and will improve information sharing practices between the private and public sectors. This will help underwriters to analyse rapidly-evolving cyber threats and risk managers to reduce uncertainty and address better solutions.

Summary

Cybersecurity and cyber risk are rapidly evolving situation. The work that the European Commission is doing on the NIS Directive and the cPPP is a crucially important one.

As a group, we should monitor the progress of cyber risk and its impact on insurance. As part of this work, we should understand the implication of the outcome of the cPPP on the Actuarial and Insurance communities. Therefore, the NLWG proposes that going forward, we update the AAE Insurance Committee on any material progress on this matter.