AMIC response: EC consultation on improving resilience of financial services against cyberattacks

19 March 2020

AMIC welcomes the opportunity to answer to this consultation on improving resilience of financial services against cyberattacks.

We understand the EC is mainly considering potential sectorial legislative changes on the basis of the ESAs opinion.

We note that this assessment by the ESAs, despite being useful, is limited to a legislative gap analysis at EU level and fails to recognise the:

- Nature of incidents reported
- Specific nature of asset management
- Cross-sectoral EU regulatory provisions: GDPR, NIS, ENISA
- Breadth of existing sectorial rules
- International standards/certifications/protocols available to regulated entities
- National regulatory provisions
- Existing industry practices

The following analysis lead us to think that sectorial legislative change for asset managers is not necessary at this stage, due to the current state of play which already ensures the appropriate practical and regulatory setup in the area of asset management.

(1) **Nature of incidents reported:** As highlighted by a report from KPMG and the IA, "the overwhelming majority of incidents suffered have involved client data theft or data loss more generally". We believe these types of incidents are already fully addressed by the cross-sectoral regulatory provisions, and notably the EU General Data Protection Regulation (GDPR), which are applicable to asset management companies among others.

(2) **The specific nature of asset management**: We would like to remind you that there are strong business incentives for asset managers to prevent and mitigate such type of events. Reputation and consumers' confidence are a pre-requisite to operate any business but in particular in the sector of asset management: "*Cyber security is, perhaps more than anything else, an issue of brand and reputation*."[1] In particular, let us remind you that asset managers are remunerated by investors paying management fees, which by nature imply a long-standing relationship with clients, based on trust.

[1] https://assets.kpmg/content/dam/kpmg/uk/pdf/2018/04/building-cyber-resilience-in-asset-management.pdf

(3) **Cross-sectoral EU regulatory provisions**: Key financial infrastructures (banks, CCPs and trading venues) but also digital service providers (cloud computing services), which asset managers are relying on, are already included in the scope of the NIS directive and need to comply with security and notification requirements. Asset managers also benefit indirectly from the more recently adopted Cybersecurity Act which will enhance cyber-resilience in the EU with the reform of ENISA and the creation of a certification framework. Finally, and most importantly, GDPR covers all firms, including asset managers, and allows NCAs to impose fines of up to 4% of global turnover for lax privacy protection.

(4) Sectorial legislation: ESMA analysis indicates that cyber-risk is de facto covered by sectorial legislation. Even if cyber-risk is not spelled out explicitly in the UCITS directive and AIFMD, cyber-risk is nevertheless part of the risks that an asset manager is already required to identify, monitor and manage. More specifically, cyber-risk is already included via relevant terminology (information, electronic data, business continuity), requirements on operational risks which cover ICT/cybersecurity risk (obligation to identify all relevant risks and manage them), governance requirements and overarching requirements for robust risk management framework applicable to cyber/ICT. We note that ESMA signalled there is no specific incident reporting requirement but would like to highlight that securities regulators, such as the AMF in France, already require it **and quote the existing EU directives (AIFMD, UCITS) as a legal basis to empower securities regulators to do so**. We would also like to remind you that under GDPR, asset managers are anyway required to notify competent supervisory authorities, in the event of a personal data breach. Based on the EU framework national supervisors have imposed a series of obligations to asset managers (organisation, compliance system, governance, risk management, outsourcing, data recording and retention) and conduct inspections to ensure that they are cyber-resilient. These inspections can lead to follow-up letters containing requests to remedy the anomalies identified. Finally, we note that ESMA has announced that it intends, in 2020, to conduct supervisory convergence initiatives in the areas of cybersecurity and cyber-resilience.

(5) **International standards/certifications/protocols already available to regulated entities:** Asset managers can already rely on international standards to design, implement, review and upgrade their cybersecurity strategy:

- NIS
- ISO standards 27001 and 27002
- COBIT 5
- CIS20

(6) **National provisions**: Key EU jurisdictions for asset managers have also adopted requirements contributing to protect all stakeholders against cybercrime. These national laws are criminalising offences against the confidentiality, integrity and availability of computer data and systems, computer-related offences, content-related offences and offences relating to infringement of copyright and associated rights. More recently, based on the cross-sectoral EU legislation applicable to cybersecurity (e.g. NIS directive), amendements have been introduced contributing to enhance cyber-resilience overall.

Among others and as an example, we can mention France, where the concept of cybercrime was initially defined in the French Data Protection Act of 1978. This concept was subsequently refined in several successive laws between 1988 (Godfrain

Act on computer fraud) and 2006 (Anti-Terrorism Act). Within this framework, in 2009 France set up the French National Cybersecurity Agency, ANSSI, in the Secretariat General for National Defence and Security. In 2018, a law, a decree, and an *arrêté* were adopted to transpose the NIS directive, contributing to identify operators of essential services, including key financial stakeholders and infrastructures.

(7) Trade associations in key jurisdictions for asset managers have adopted best practices and codes of conduct, such as this non-exhaustive list of examples:

- The IA and KPMG's report on building cyber resilience in asset management
- AFG's Practical Guide, factsheets and surveys
- BVI's Guide to Cyber Security