# ABOUT THE COMMITTEES

**Retail Committee**

The retail sector is today faced with a host of issues that impact on its information systems security processes. In this era of GDPR, traceability and consumer demands, how do we monetise our customer data while guaranteeing that the data we collect is safe? How do we integrate the new payment methods into our business processes and information systems? What implications does omnichannel have for business and what impact will it have on information system security? Lastly, what lessons can be learned from the new purchasing experiences that threaten some existing models? The members of this Committee are there to share their views on these issues and contribute their suggestions and recommended approaches to the debate.

**Industry Committee**

In a context subject to profound and far-reaching change, how can we reconcile agility, security, responsibility, a transversal approach, openness to partners and budgetary constraints while taking into account the business issues relevant to the sector? This Committee's purpose is to examine:

- The CISO's contribution to digital transformation (adapting to new issues and business models; the extension and opening up of the information system; agility of the industrial information system, etc.).
- The obstacles and constraints with which the industrial sector must come to terms.
- The different partners' views of these issues and the way they drive development of their offers and technologies to solve their customers' problems.

**Banking and Insurance Committee**

The purpose of this Committee is to produce a 3-to-5-year assessment forecast of the IT/security issues relevant to the banking and insurance industries to enable participants to anticipate forthcoming challenges by planning their future development. With this in mind, the Committee has identified several areas appropriate for discussion:

- Understanding the legal requirements
- Controlling third parties
- Assessing the maturity of the players involved
- Benchmarking frameworks
- Managing MSSPs
- The public cloud (how to ensure a view of continuity throughout the chain)
- Cyber resilience

**Public Sector Committee**

- The role of this Committee is to address a number of key points regarding information system security in the public sector:
- How do we raise awareness among citizens and offer them practical solutions?
- How do we enhance the role of information system security within the public sector? (Through a common skills and professions reference framework?)

- What options do we have for pooling resources between different departments of state?
- Working to increase awareness of digital security at all levels of the public sector/civil service
- How do we ensure that public procurement is a positive lever for the cybersecurity industry, particularly with respect to start-ups?
- What is the best way to share expertise between ministries?
- How do we ensure that decisions taken centrally filter down to public servants at regional and local level?

**Governance Committee**

The main purpose of this Committee is to address 3 topics related to governance:

- GDPR: the day after

What have the parties involved achieved? / What has driven and what has obstructed compliance? / How has GDRP helped establish a corporate data governance policy? / How have your companies worked with subcontractors?

- What attitude to new threats?

Planning for DDoS attacks through the IoT / How to deal with attacks on cloud services / How to combat malware that targets business applications / How do we raise awareness among employees? / Is cyber insurance one way of allowing for the impact?

- And when a crisis occurs: how do we protect our business through ultimate resilience?

How do we prepare for a crisis? / How resilient can a dependent IS company be? / How do we tackle the subject of the ultimate crisis with all the company's BUs? How can we ensure that cyber first is the new watchword?