Business as usual

54%

suffered from a cyber attack in the past 12 months, of which 44% had to deal with disruption of business processes. Malicious software, social engineering and phishing are the most usual methods.

Insider threat

80% of respondents do not have a proper insider threat management program; in particular, they do not have technical monitoring of suspicious activities (named by 60%), appropriate data classification (51%) and multidisciplinary coordination (49%).

Working on response capabilities

60% have a cyber response plan, and they tend to be satisfied with the effectiveness, resources and know-how in this domain (2015: 55%). 82% of them normally review this plan as part of their yearly review cycle.

Third-party risks

93% of FS institutions require right to audit, and 65% of NON-FS institutions require right to audit in third-party contracts.

100% of NON-FS institutions require third parties to notify cyber incidents, while 79% of FS institutions insist on it.

33% of FS institutions report that understanding, visibility and control of Cyber Security has worsened when outsourcing to third parties, while only 8% of NON-FS institutions report this.

Key Findings

Perception of cloud

81% of FS institution respondents believe that leveraging cloud technology will not reduce security while only

46% of NON-FS institutions state the same.

The 4th industrial revolution challenge

53% do not have an overview of Internet of Things devices. Approximately one third of respondents that say the Internet of Things is relevant to them do not leverage the concept of security by design.

Join forces

95% were looking for more cooperation in 2015. One year later, 66% say that they have actually done that. Sharing threat intelligence (named by 88%), sharing lessons learned (83%) and sharing preventive measures (78%) are the most common goals of collaboration.

Lack of insight

38% do not have any method of measuring cyber risk, which is a slight deterioration compared with 2015 (44%). Awareness of the damage significantly improved: 17% of large companies lack insight into the damage caused by cyber attacks (2015: 50%).