Key findings

Cyber attacks are increasing

88% of respondents suffered a cyber-attack in the past 12 months (2016: 54%).

56% had to deal with a disruption of business processes (2016: 44%), 37% with reputational damage (2016: 24%), 36% with financial loss (2016: 36%) as a consequence of cyber attacks.

A deeper understanding of cyber risks is evolving

81% confirm that they have gained a deeper understanding of cyber risks in the past 12 months.

52% have gained better understanding of the attacker's motivation, strategy, and tools, 44% state that their prediction capabilities have improved.

The human factor in Cyber Security

65% confirm that their organization does not systematically work on cyber security measures that are user-friendly.

11% involve a UX specialist to achieve user-friendly security design.

Cyber Security and product/ service design

48% embed cyber security measures systematically in product/service design processes compared to 65% embedding data protection/privacy measures.

IoT concerns

59% state that their main concerns regarding IoT-related risks are exotic devices that are introduced in the organization's network and the fact that traditional controls are no longer effective (also 59%).

Struggling with Internet of Things (IoT)

48% include IoT or operational technology (OT) assets in their cyber security strategy and policy.

33% report that they have gained better insights into the landscape of the relevant IoT devices in the past 12 months.

31% have an overview of IoT and operational technology (OT) devices deployed in their organization, 35% did not try to get an overview in the past 12 months (2016: 53%), 17% tried to get an overview, but did not succeed.

Slow anticipation of artificial intelligence

43% believe that the rise of AI will lead to new challenges in cyber security within 2–3 years, while only 26% think that the rise of AI leads to new challenges in cyber security now.

12% analyze the security impact of potential AI use cases systematically.

4% use AI to protect themselves from cyber threats, but 40% expect that AI is going to be used by attackers in the future.