ESMT Annual Forum 2016

“Digitalization. Responsible strategies for business and society”

Panel 1

Security and Privacy. New Risks for Management and Innovation

The panel discussed the global challenges of cyber security for corporations and governments. Despite significant progress in cyber security strategies, the panel agreed that a greater focus within organizations on risk assessment and security management is still required.

With the growing reliance on data for growth and innovation, companies have a responsibility to users to protect privacy. Frédérick Douzet argued, “This needs a good system for management and extensive training for the workforce because business model depends on it.” Cyber requirements vary greatly across companies and sectors. For Sandro Gaycken, this represents a new paradigm, “The process for finding out what each company needs is still in its infancy with cyber security products being until recently mostly about marketing rather than real technological developments.”

Whilst spending on cyber security has increased exponentially, the effectiveness of cyber defenses is difficult to measure. Jamie Shea suggested organizations should focus on better base-line assessment of where the risks are and what is essential for an organization to protect, rather than on buying ‘miracle’ products without understanding what is required. A point reiterated by Stefan Heissner, who said, “The push for technological innovation and market growth has failed to drive research and development into security elements.” He also argued that better regulation would see governments creating a framework for companies to do better.

The panel was aligned that there needs to be greater exchange across companies, sectors, and countries. In the absence of a comprehensive global strategy for improving cyber security, organizations discussing challenges, and sharing methodologies for risk assessment, good management experiences, and training processes could help avoid future costly failures. Melissa Hathaway shifted the focus onto outcome over activity, emphasizing that the effectiveness of information sharing should be measured against what organizations and countries want to achieve. She also referenced the geopolitical aspect of the debate. “It comes down to a geopolitical equation. State leaders understand that strong cyber security results in global strength and power. It’s a competition for this.”

Frédérick Douzet introduced the dimension of responsible leadership, highlighting how organizations must be clear on who is responsible in the instance of an attack. In all organizations, people have to know their role in protecting cyber security. In banks, leadership implements training and exercises across staff, with the result that banks are more secure than utility companies. According to Melissa Hathaway, “We need to start thinking forward. Industry 4.0 - fit bits, embedded medical devices, the Internet of Things - these products are not designed with security embedded and are connected to whole host of other systems. Right now, we’re blinding adopting the technology without thinking about security, safety, privacy, and resilience. Everyone is at risk. But we can do it responsibly, so let’s do it now.” The panel confirmed this sense of urgency with Jamie Shea concluding that, “With privacy issues - as with climate change - we either get grip on it within the next 10 years or we’ve lost.”