

Digitalisation & cybersecurity

From Cyber quantification to Cyber enforcement plan, with C-Level

Steven Lafosse Marin
Head of Sales Private Sector
Airbus Defence and Space Cybersecurity

Digitalisation becomes transversals

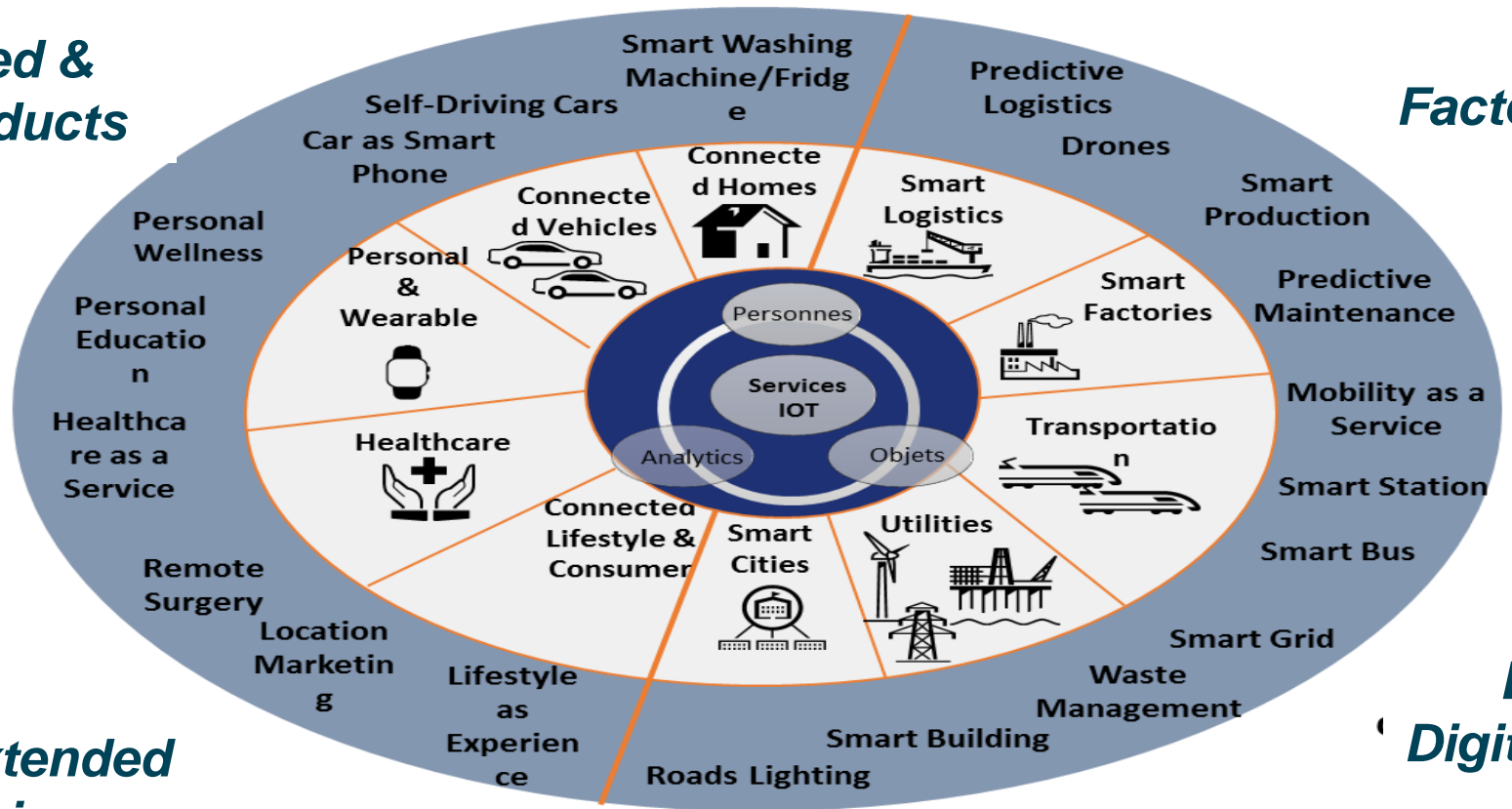
Connected & Smart Products

Factory 4.0

Supply chain

Data and Digital platforms

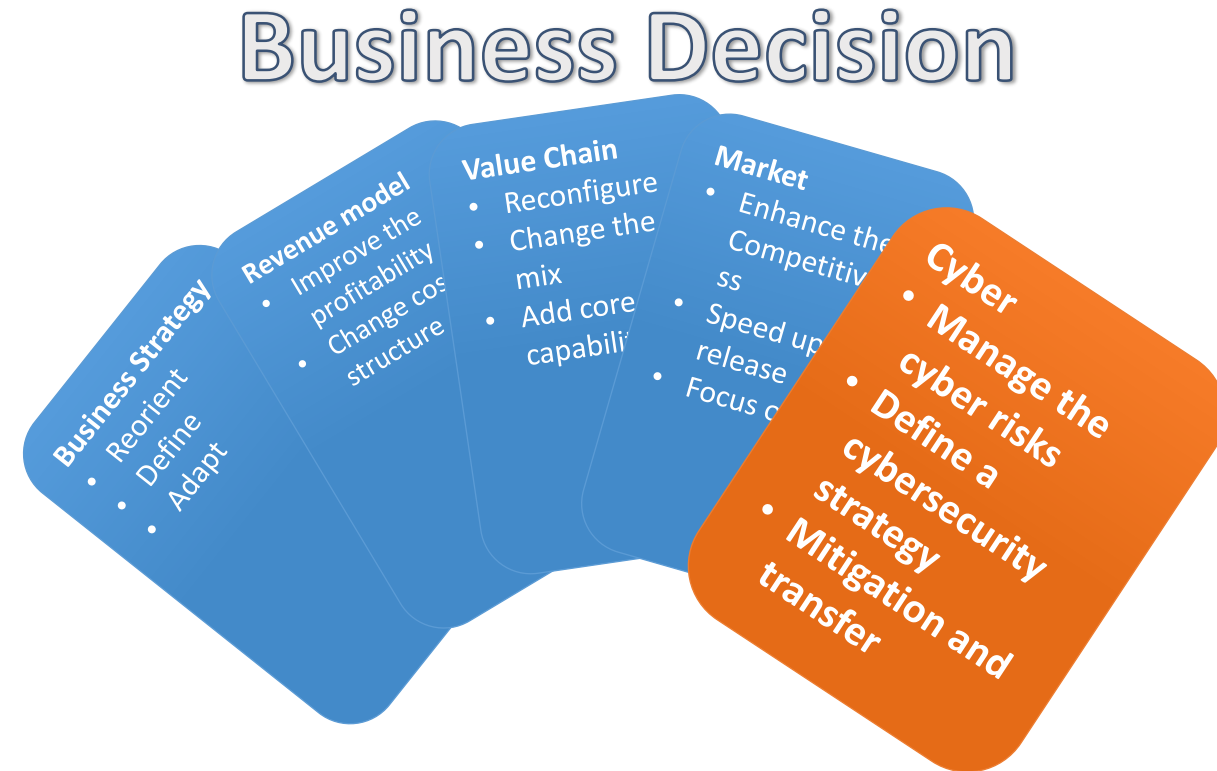
Cloud & extended Enterprise



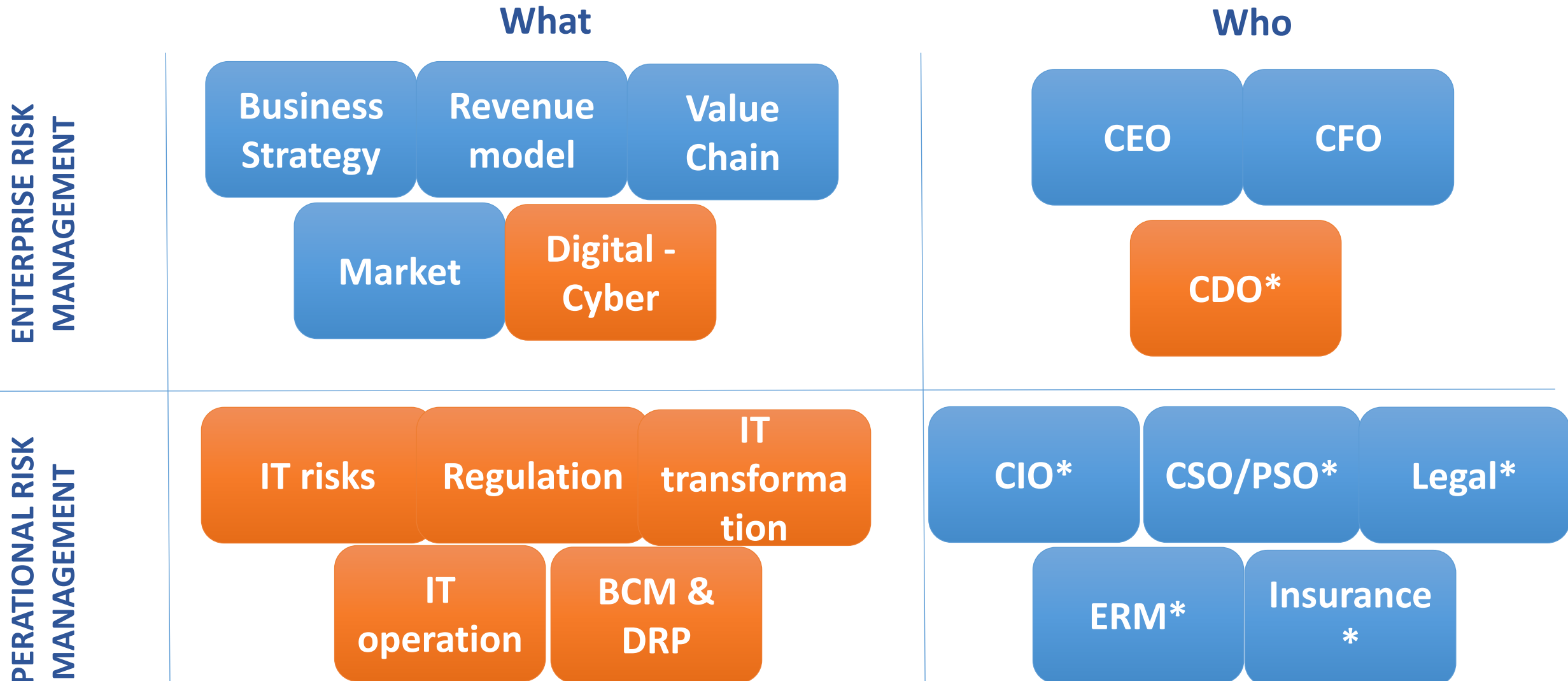
Technology core & analytics core
 Application/Industry Clouds
 Smart Services

C-Level needs to realign enterprise strategy due to digitalisation and cyber risks

- 1) **Cyber becomes an enterprise risk vector**
 - Trends: Global digitalisation, Factory 4.0
 - Cyber can't be managed only from a technical and operational perspective
- 2) **C-Level needs support in order to take decision regarding /or implying Cyber**
 - Business decision
 - Cybersecurity strategy
 - Cyber Insurance
 - Investment
- 3) **C-Level needs financial figures to quantify cyber risks**

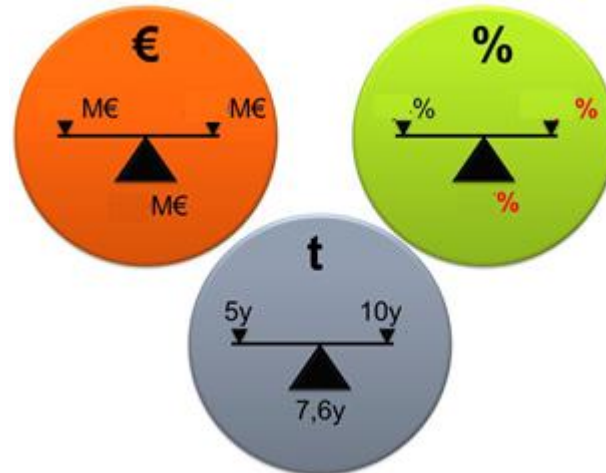
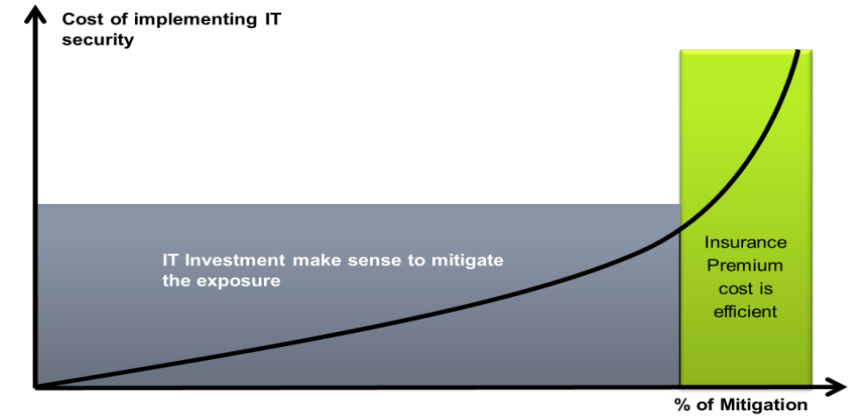


Cyber risk management ecosystem



CyPREs RM initiative, innovative methodology, on standardization process, a strategic vision for Top Exec customers

Consolidated results for C-Level, rationalize and prioritize budgets, Then manage the cyber risks at the operational level



Combination between Cyber investment and Cyber insurance

Scientific support (IRT-System-X,...), international institutions (OECD, DG Connect, FERMA), ANSSI (French cyber agency) and business customers



On the one hand, cyber is clearly a risk, especially on the board agenda. On the other, about what insurance covers and whether it using language and definitions within cyber is common among insurance buyers over the business, as well as worries over the security major talking points at the recent Advisian

Cyber risks: the SPICE Initiative at Airbus
Philippe Cotelle, Head of Insurance Risk Management, Airbus Defence and Space



There are three main obstacles to a good understanding of cyber risks in our organisations, which I believe are common to most businesses.

It is a pilot programme for a business impact analysis to identify cyber-related disaster scenarios that could affect our operational capability and it is truly innovative.

SPICE needs high level technical experts who know the cyber threat environment of the organisation. To start, we gathered representatives of all the functions as well as from IT and information management security to:

- Educate the operational managers to the new cyber threats;
- Discuss the security issues with great care;
- Openly consider some potential cyber attack scenarios – and not assume it could not happen to us;
- Support 'impacted' functions and information management security.

Building the scenario

Attacks: We focussed on identifying potentially catastrophic scenarios:

- Who might attack us and what would their motives be?
- What functions and assets would be impacted?
- How would we recover and how long would it take?

Cost: We calculated the business and operational impact with some key scenarios.

To get over these obstacles, the risk manager has to be able to demonstrate to the CEO or the executive committee the possible financial impact of a massive cyber attack in terms of business interruption and loss of business opportunity for this the risk



Digitalisation, Business and efficiency

People Buy
From People
They Trust

Cyber, Trust and Confidence