

How to develop strategies for facing cyberrisks?

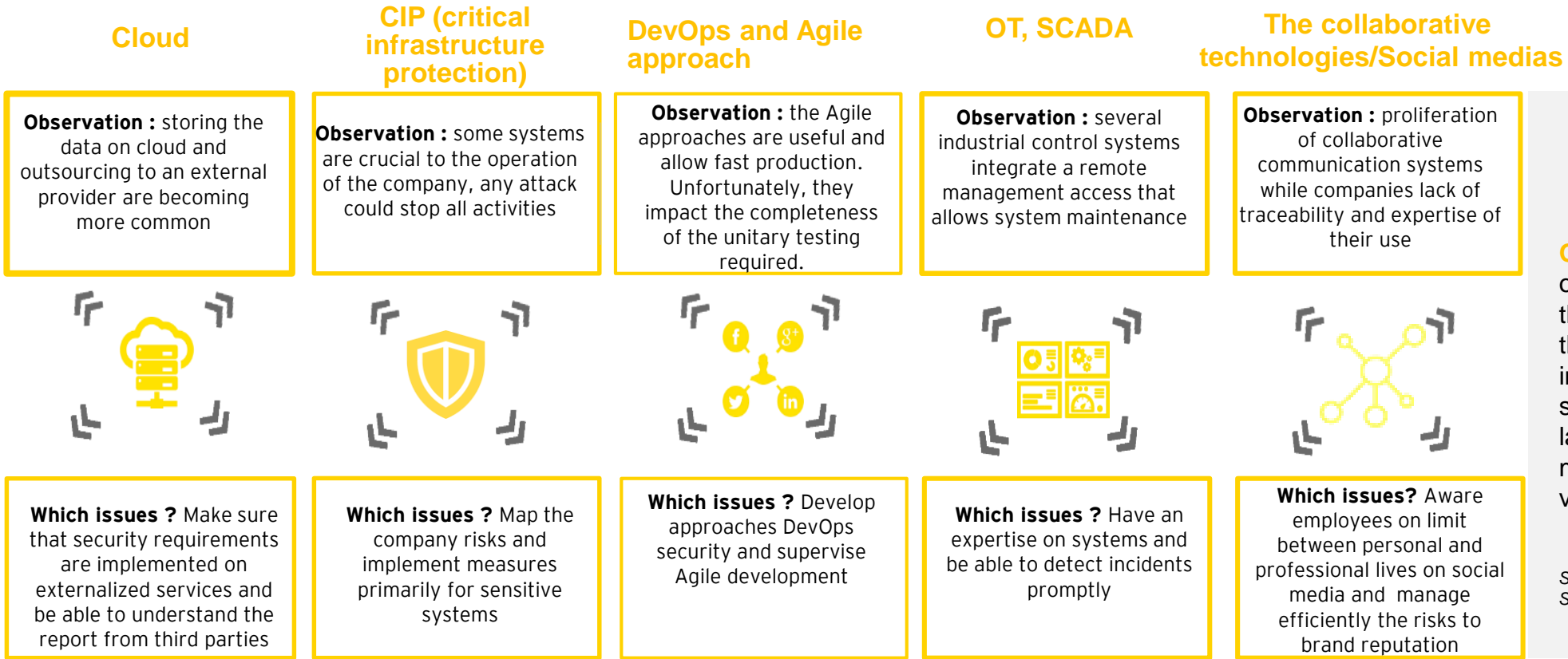
Laurent Peliks, Partner EY

**Safe and Ethical Cyberspace, digital assets and risks:
*How to assess the intangible impacts of a growing phenomenon?***

The World Conference on Intellectual Capital for Communities

UNESCO, June 14&15 2018

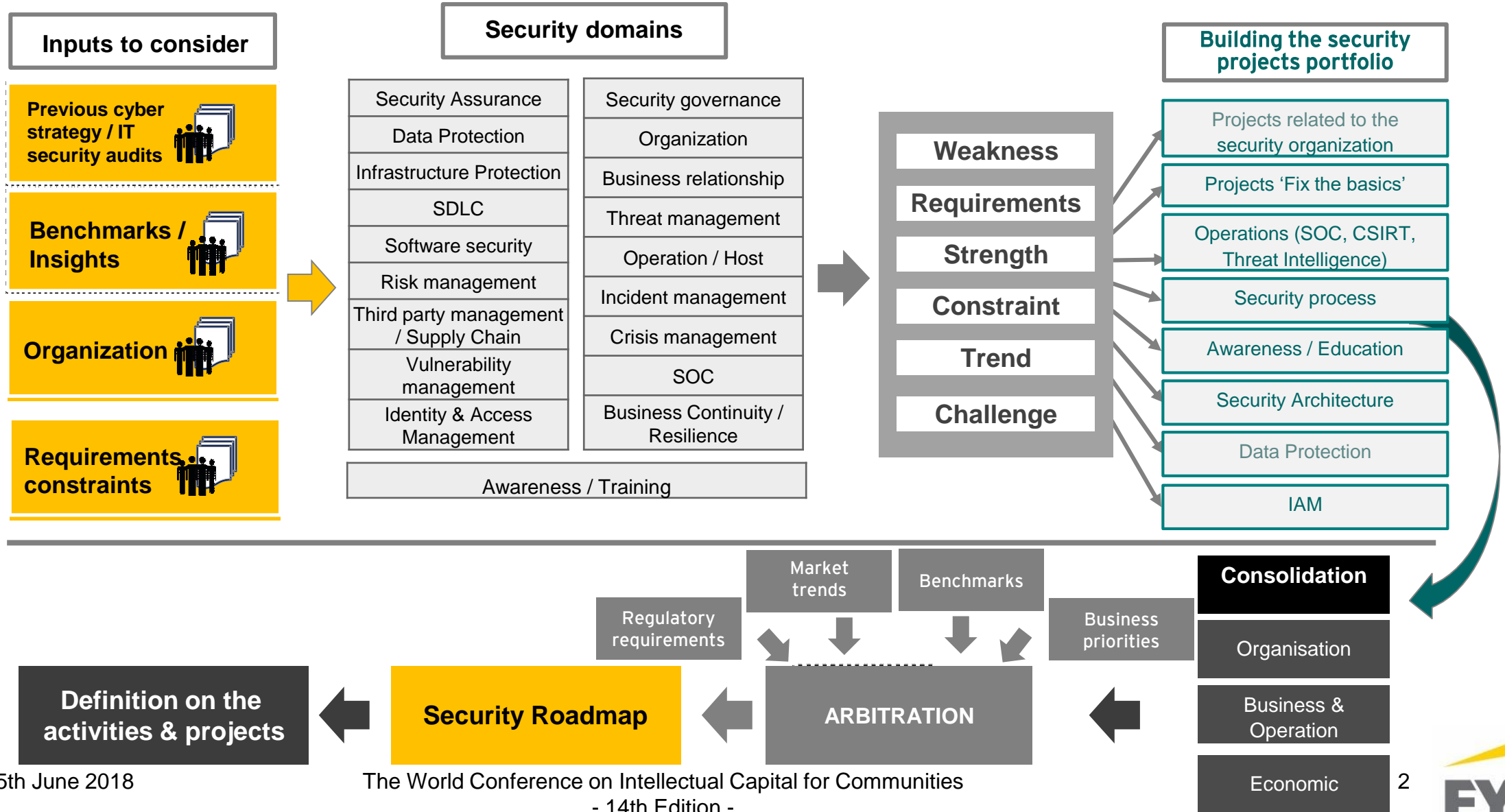
Cyberrisk landscape : New challenges & issues



Only 4% of organizations are confident that they have fully considered the information security implications of their current strategy, and that their risk landscape incorporates and monitors cyber threats, vulnerabilities and risks.

Source : EY, Global Information Security Survey, 2017-2018

Developing cyber strategy in a nutshell...



Understanding its ecosystem & maturity level is the key



1

Identify high-value assets and critical information



2

Qualify the cyber threat exposure



3

Identify the cyber attack tactics



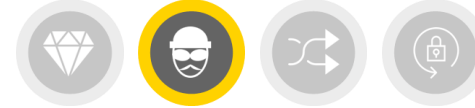
4

Define the adapted cybersecurity response plan

Focus on crown-jewels: sensitive information & IT assets



- What are the sensitive processes associated with your business line that are subject to attacks or fraud?
- What are the information assets and the information system related to these processes?
- What are the different actors (internal and external) that can interact with this assets?

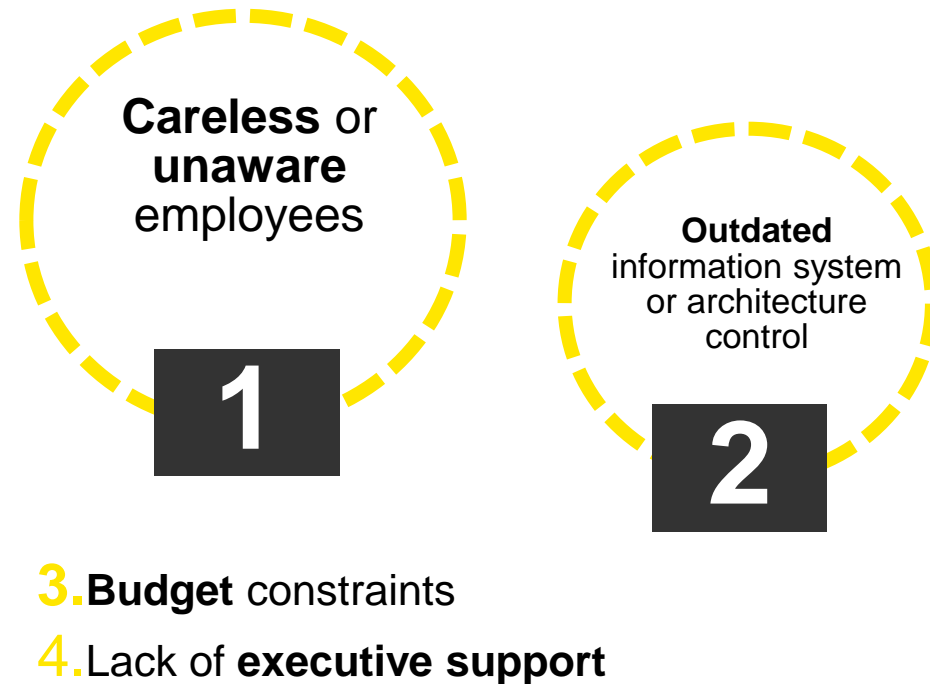


Focus on cyber threat & vulnerabilities

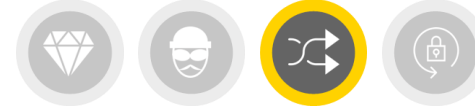
Main cyber threats

- 1 ✓ Financial Fraud
✓ Unavailability of operations capacity due to cyber attacks on industrial equipment
- 2 ✓ Cyber criminality based on Ransomware or 0-days attacks
- 3 ✓ Financial information / IP or data steal (employees / 3rd party)
- 4 ✓ Security impact caused by a migration to the Cloud or a digital transformation, without considering security aspects

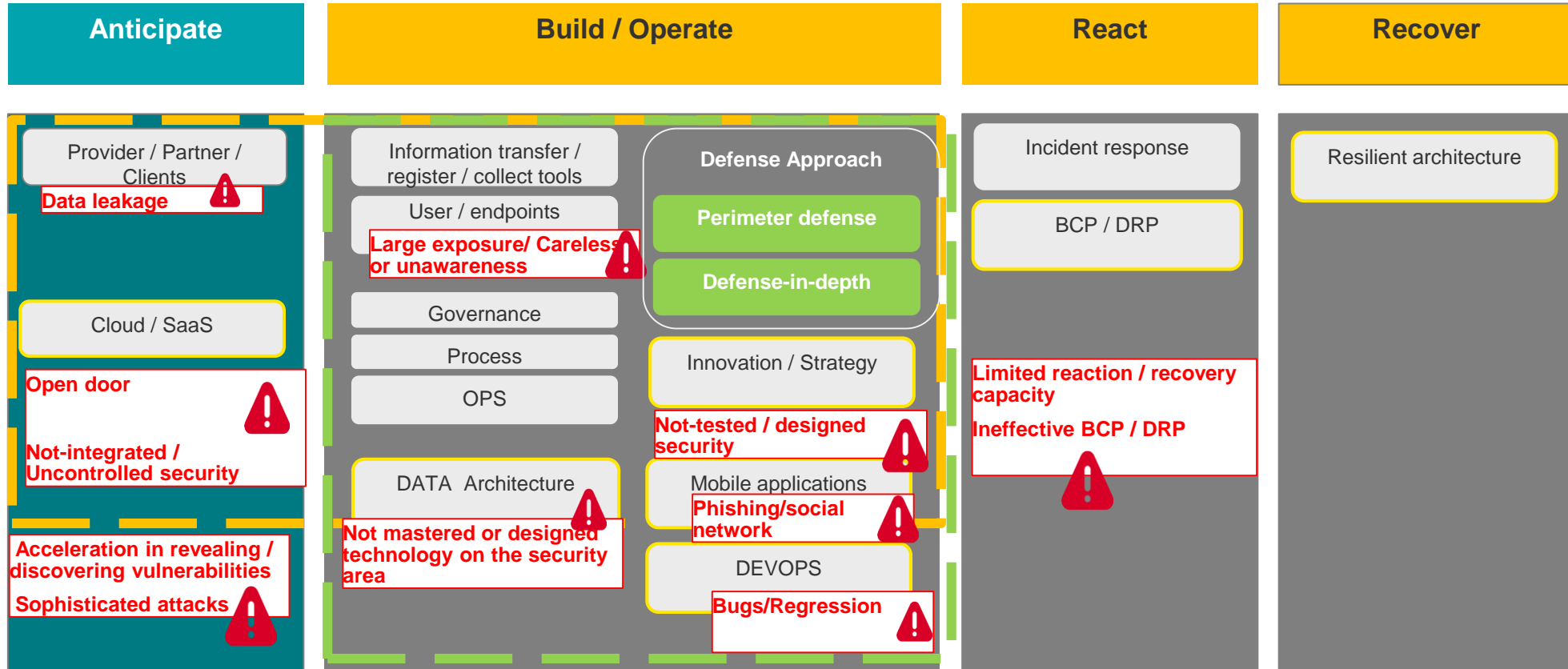
Main Cyber vulnerabilities



Source: EY Global Information Security Survey 2017-2018



Focus on cyberattack & preferred target





Focus on security roadmap

