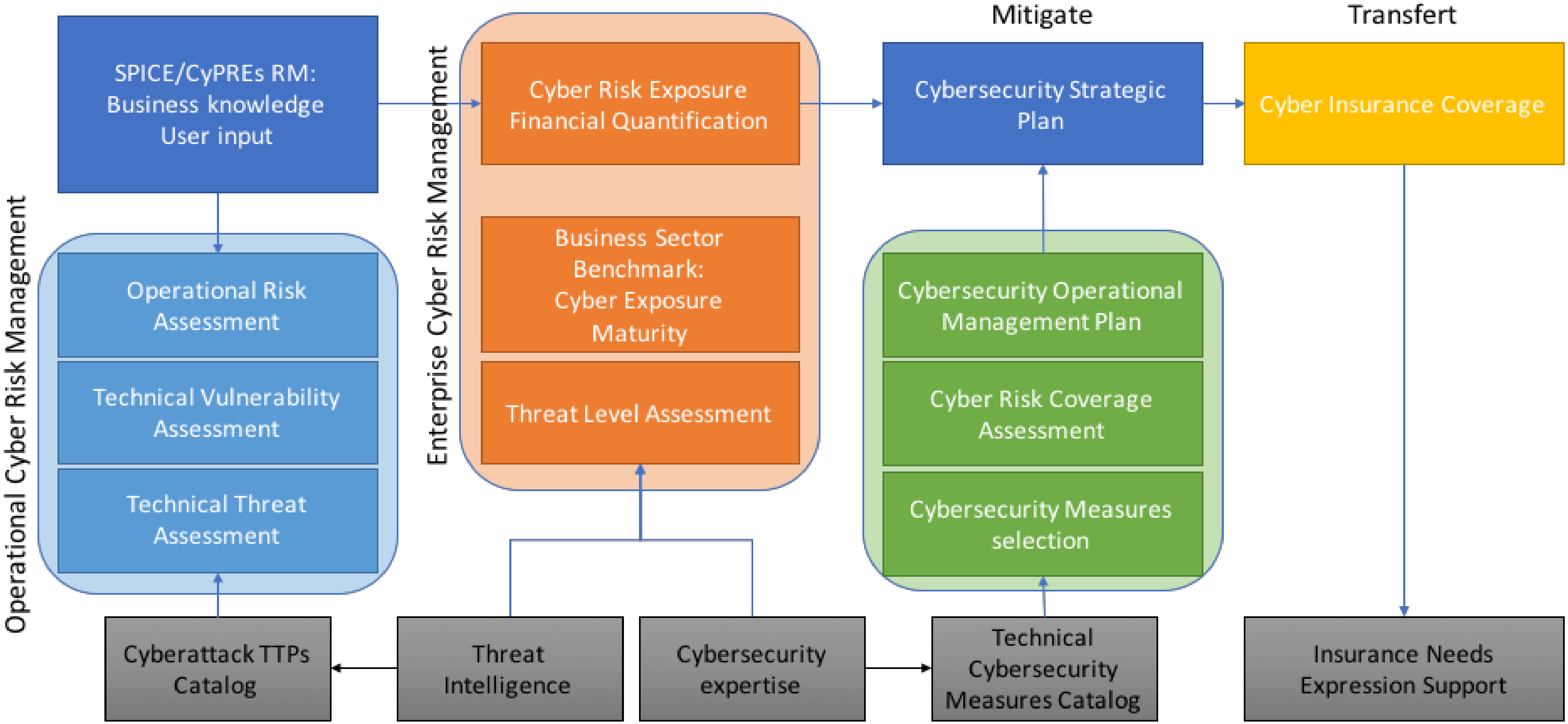
Cyber Risk Governance
Strategic Risk Analysis

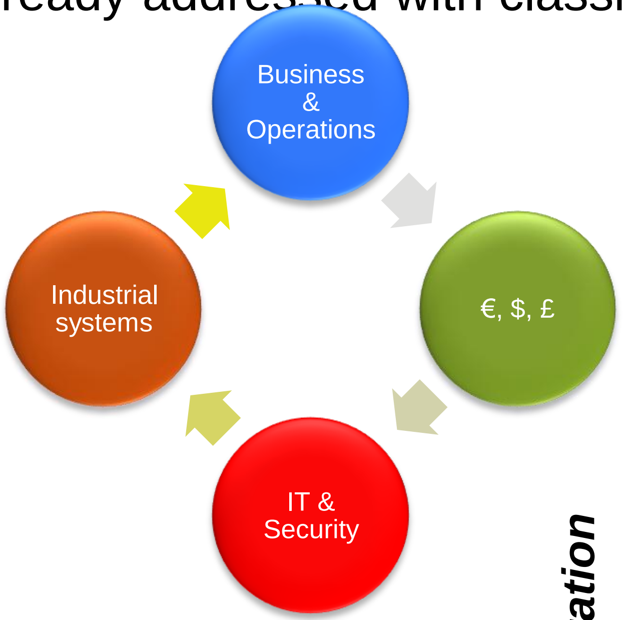
Philippe Cotelle
Head of Insurance Risk Management
Airbus Defence and Space

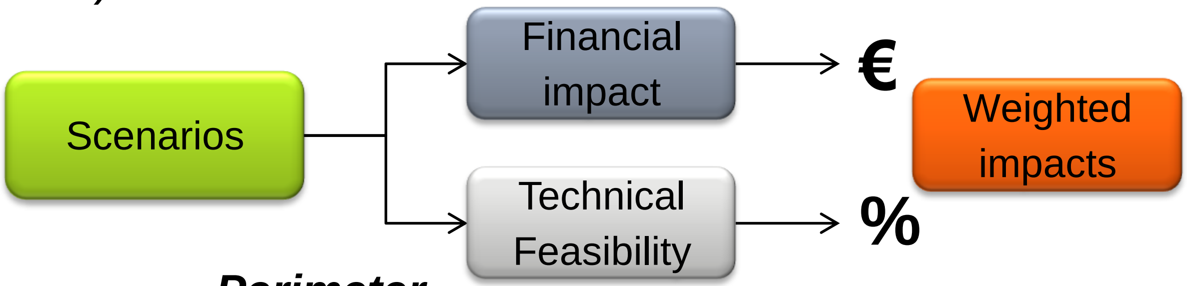
CYBERSECURITY RISK MANAGEMENT FRAMEWORK

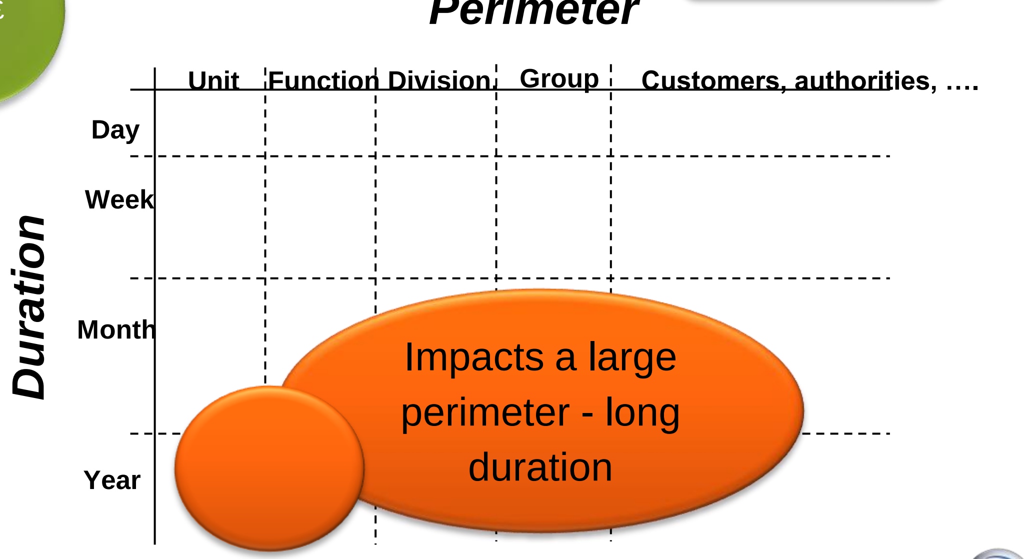

Mitigate
Transfert
SPICE/CyPREs RM:
Business knowledge
User input
Operational Cyber Risk Management
Operational Risk Assessment
Technical Vulnerability Assessment
Technical Threat Assessment
Enterprise Cyber Risk Management
Cyber Risk Exposure Financial Quantification
Business Sector Benchmark: Cyber Exposure Maturity
Threat Level Assessment
Cybersecurity Strategic Plan
Cybersecurity Operational Management Plan
Cyber Risk Coverage Assessment
Cybersecurity Measures selection
Cyber Insurance Coverage
Cyberattack TTPs Catalog
Threat Intelligence
Cybersecurity expertise
Technical Cybersecurity Measures Catalog
Insurance Needs Expression Support

A bottom-up approach to better grasp cyber risk impacts

Define your risk exposure by leveraging all the necessary functions of the company and focus on the maximum foreseeable loss (low intensity risks are already addressed with classical means)

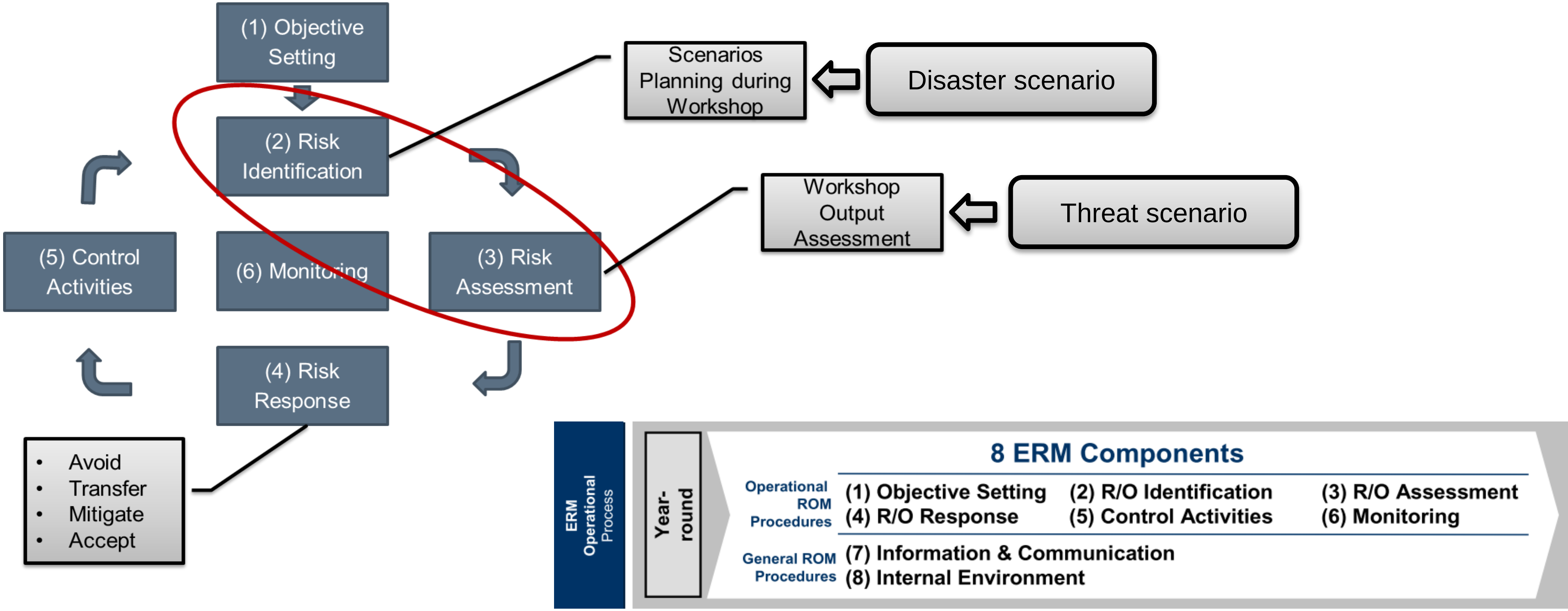





Perimeter
Unit
Function
Division
Group
Customers, authorities, ….
Duration
Day
Week
Month
Year
Impacts a large perimeter - long duration

SPICE – Approach (Methodology)

Feeding into the standard enterprise risk management process, focusing on ERM components **(2) Risk Identification**, **(3) Risk assessment** and also identifying potential responses for **(4) R&O Response**



(1) Objective Setting

(2) Risk Identification

(3) Risk Assessment

(4) Risk Response

(5) Control Activities

(6) Monitoring

Scenarios Planning during Workshop

Disaster scenario

Workshop Output Assessment

Threat scenario

- Avoid
- Transfer
- Mitigate
- Accept

ERM Operational Process

Year-round

8 ERM Components

Operational ROM Procedures
(1) Objective Setting (2) R/O Identification (3) R/O Assessment
(4) R/O Response (5) Control Activities (6) Monitoring

General ROM Procedures
(7) Information & Communication
(8) Internal Environment

SPICE initiative

(Scenario Planning to Identify Cyber Exposure)

A program for Business impact analysis to identify disaster scenarios affecting our operational capabilities related to a cyber-event

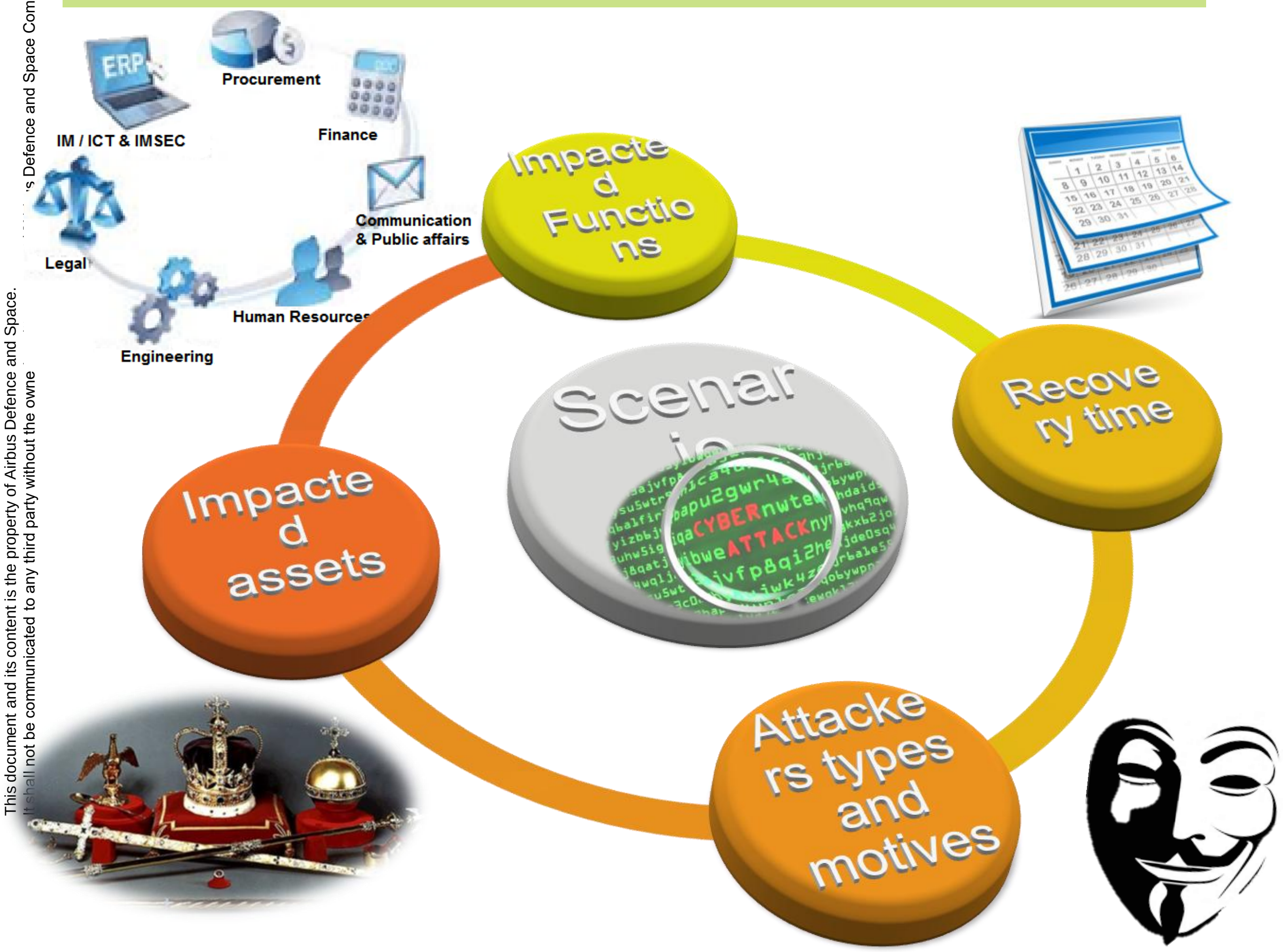
Gathering representatives of all the functions as well as IT and IM Security to overcome 3 hurdles :

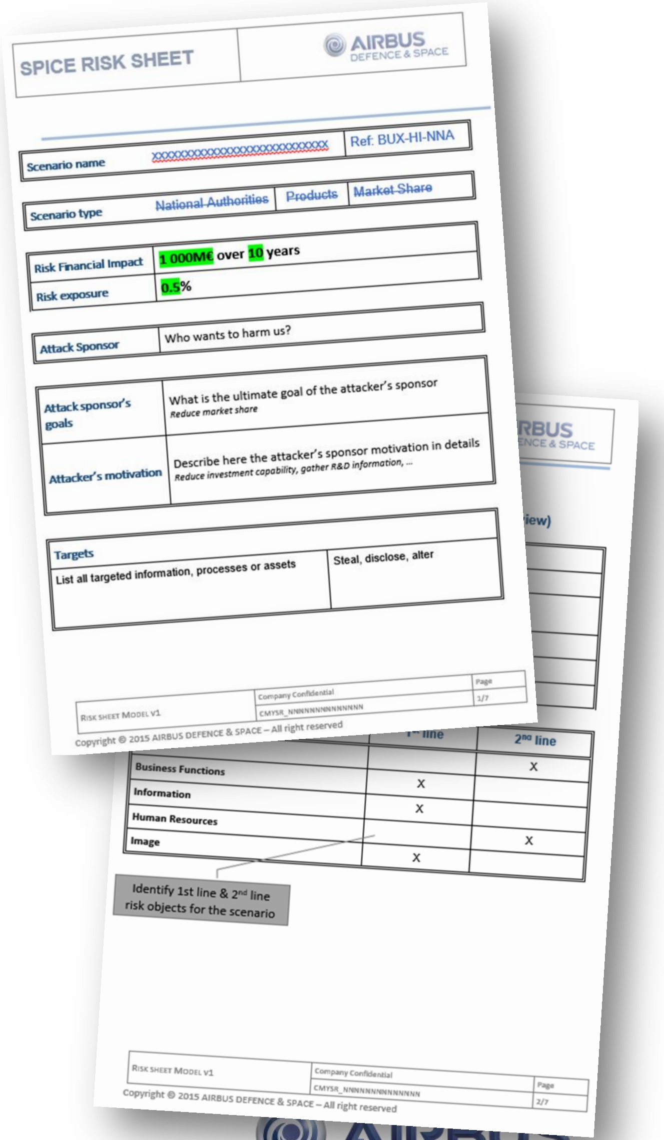
- Explain to the operational people that we need them
- Address the security issue with extreme care,
- Be prepared to openly discuss some potential scenarios of exposure. No company shall assume that it is impossible to be hacked.

Scenarios identification

Scenario identification

- Focus on catastrophic scenarios
- Including clear hypothesis




SPICE RISK SHEET

Scenario name	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Ref: BUX-HI-NNA

Scenario type	~~National Authorities~~	~~Products~~	~~Market Share~~

Risk Financial Impact	1 000M€ over 10 years
Risk exposure	0.5%

Attack Sponsor	Who wants to harm us?

Attack sponsor's goals	What is the ultimate goal of the attacker's sponsor *Reduce market share*
Attacker's motivation	Describe here the attacker's sponsor motivation in details *Reduce investment capability, gather R&D information, …*

Targets	
List all targeted information, processes or assets	Steal, disclose, alter

Risk sheet Model v1 | Company Confidential | Page
CMYSR_NNNNNNNNNNNNNN | 1/7

Copyright © 2015 AIRBUS DEFENCE & SPACE – All right reserved

…iew)

	1st line	2nd line
Business Functions		X
Information	X	
Human Resources	X	
Image		X
	X	

Identify 1st line & 2nd line risk objects for the scenario

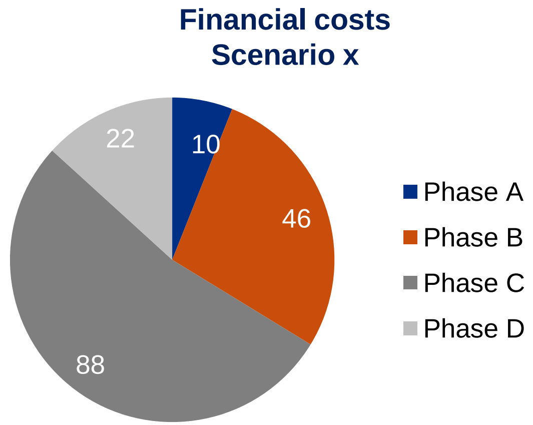
Risk sheet Model v1 | Company Confidential | Page
CMYSR_NNNNNNNNNNNNNN | 2/7

Copyright © 2015 AIRBUS DEFENCE & SPACE – All right reserved

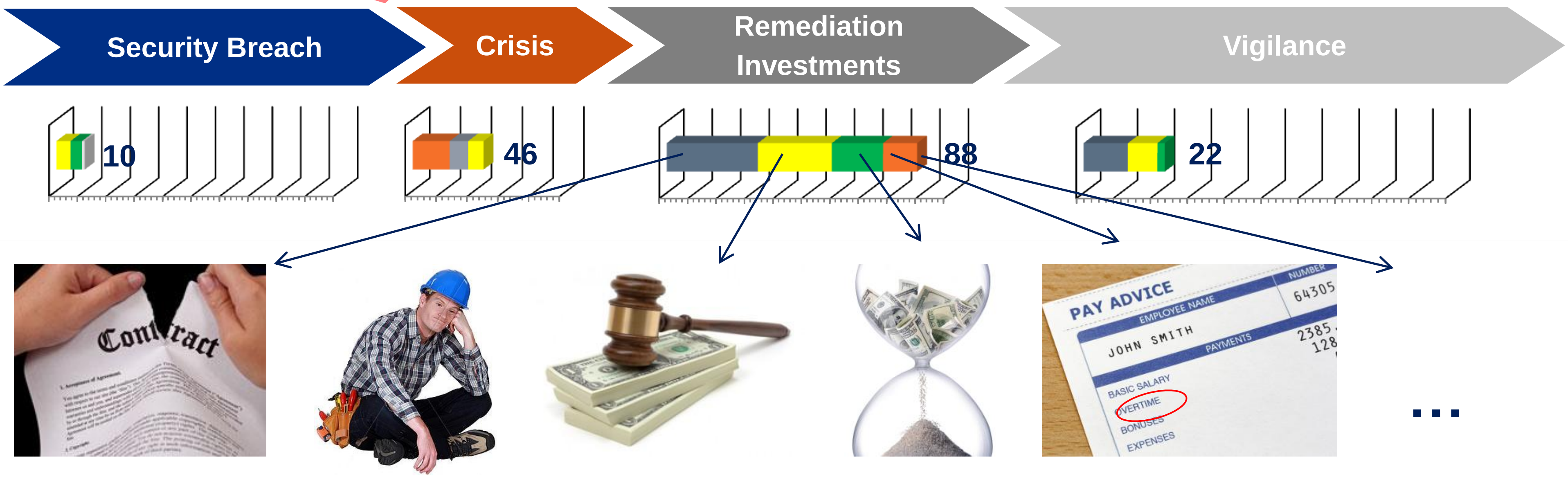
Assessing financial costs

Assessing financial cost of each scenario

- Split scenarios in 4 different phases
- Simplify the list of impacted functions
- Compute over/under charge per scenario, per phase



Security Breach Detection



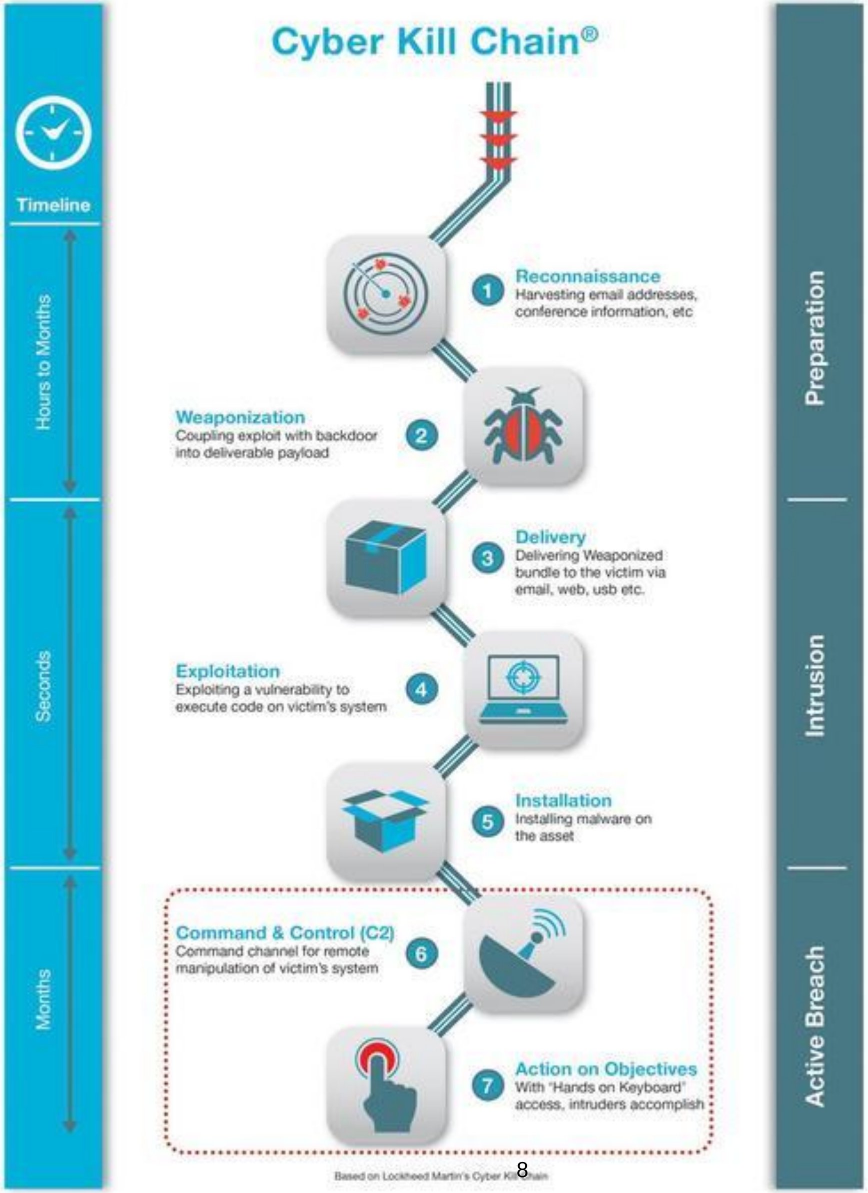
Evaluate probability of occurence

Quantify the technical probability of success of a scenario to occur

- For each step of a given scenario, identify technical ways to proceed
- Rate each step with a probability of occurrence (using internal probability scale)

Assessment performed by the local Information Management Security

APT Kill Chain description used in the technical threat scenario


Cyber Kill Chain®
Timeline
Hours to Months
Seconds
Months
Preparation
Intrusion
Active Breach
1 Reconnaissance
Harvesting email addresses, conference information, etc
2 Weaponization
Coupling exploit with backdoor into deliverable payload
3 Delivery
Delivering Weaponized bundle to the victim via email, web, usb etc.
4 Exploitation
Exploiting a vulnerability to execute code on victim's system
5 Installation
Installing malware on the asset
6 Command & Control (C2)
Command channel for remote manipulation of victim's system
7 Action on Objectives
With 'Hands on Keyboard' access, intruders accomplish
Based on Lockheed Martin's Cyber Kill Chain

APT Kill Chain description used in the technical threat scenario and rating

		Explanations
1	Business Intelligence & reconnaissance	This step consists of an information gathering targeting specific people. This is done through OSINT like social network (either profesional or not).
2	Weaponization & delivery	This step consists of the design & development of the dedicated malware set used for the attack (including social engineering materials) then of the delivery of the malware payload in the targeted environment. To be successful the attackers need information regarding the targeting systems.
3	Exploitation, priviledge escalation & C&C	This step consists of the successful malware activation. Often it relys on the active participation of the user. Then, it consists of the consolidation of the attacker position in the targeted IT environment. It is usualy done by using software vulnerability. Then, it consists of the implementation of a communication channel enabling real time attackers actions on the compromised system.
4	Lateral movement	This steps is optional and consists of the search of the primary target. The attacker will move in the targeted IT environment either to reach high value IT assets (like DC) or High value business assets. If this step is needed, either you use only one step, or you add another one depending on the difficulty of this step implementation.
5	Action	This steps consists of the search and exfiltration of the targeted information, and/or in the vandalism of key ressources. (according to the scenario definition

Rating compliant with ERM approach

Qualitative Impact Level	
4	Very High
3	High
2	Medium
1	Low
0	No impact

Probability of Occurence		
5	Certain (100%)	100%
4	Nearly certain >75%	90%
3	Likely (>50%-75%)	65%
2	Low probability (>25%-50%)	35%
1	Unlikely(<25%)	10%

[redacted]

Assessing financial costs
Lessons learned

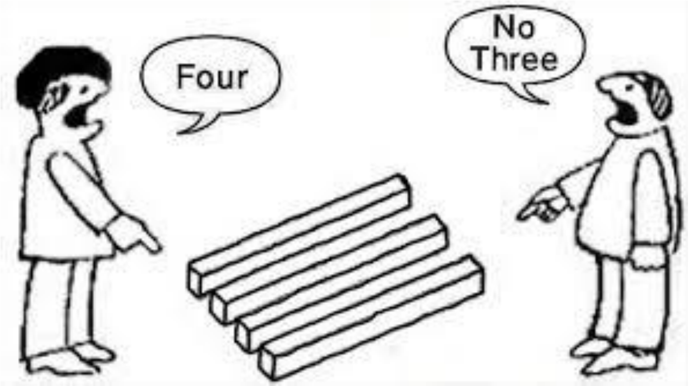
- NUMBERS are related to our financial exposure
- There is no final number
- Management has to play a role
- The objective is to reach a consensus:
  - acceptable by everyone
  - valid for our analysis

Evaluate probability of occurrence
Lessons learned

The same method was applied in the same way by experts from different sites which led to very **different numbers**.

2 different approaches:

Given the defence systems in place, in order to be successful the attacker should gather so many different skills and resources that this was very unlikely to be plausible.
As such the probabilities were therefore very low.



If an attacker was seriously considering seriously hacking a major company, then this must be a very strong organisation which in itself should have gathered all those unique skills and resources. Therefore their probabilities were more important.

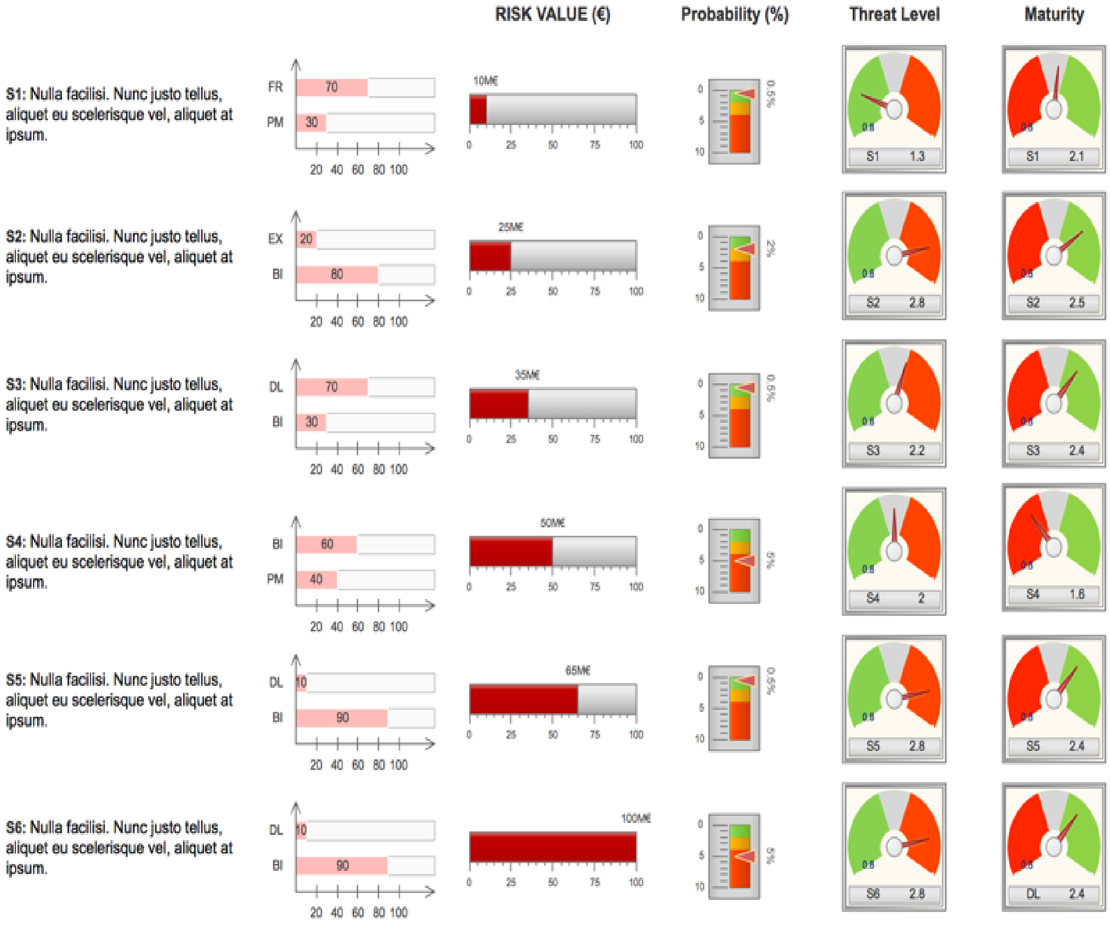
If we really want a process which gives valuable information, we need an homogeneous approach AND also to attach to each scenario the type of hacker and their motives

And why would they perform this scenario?

SPICE FOR THE BOARD

Analysis and recommendations examples:

- S2: High threat level with low risk value, low probability at 2% and good maturity level
  - Recommendation: Risk acceptance
- S4: Average threat level with medium risk value, probability at 2% and low maturity level
  - Recommendation: Risk Mitigation for Business Interruption and Product/Service Manipulation in order to increase the maturity level by improving detection and response capabilities
- S6: High threat level with high risk value, high probability at 5% and good maturity level
  - Recommendation: Risk Mitigation for Business Interruption and Data Loss in order to lower the probability by improving the protection capabilities.



S1: Nulla facilisi. Nunc justo tellus, aliquet eu scelerisque vel, aliquet at ipsum.

S2: Nulla facilisi. Nunc justo tellus, aliquet eu scelerisque vel, aliquet at ipsum.

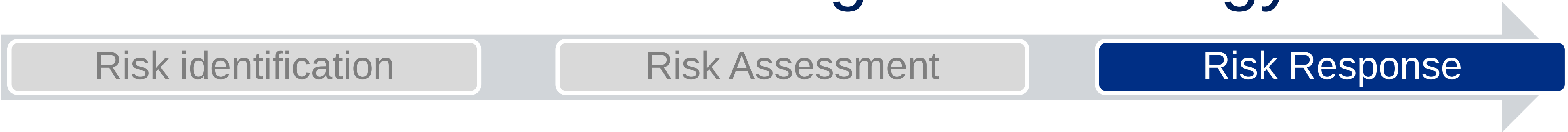
S3: Nulla facilisi. Nunc justo tellus, aliquet eu scelerisque vel, aliquet at ipsum.

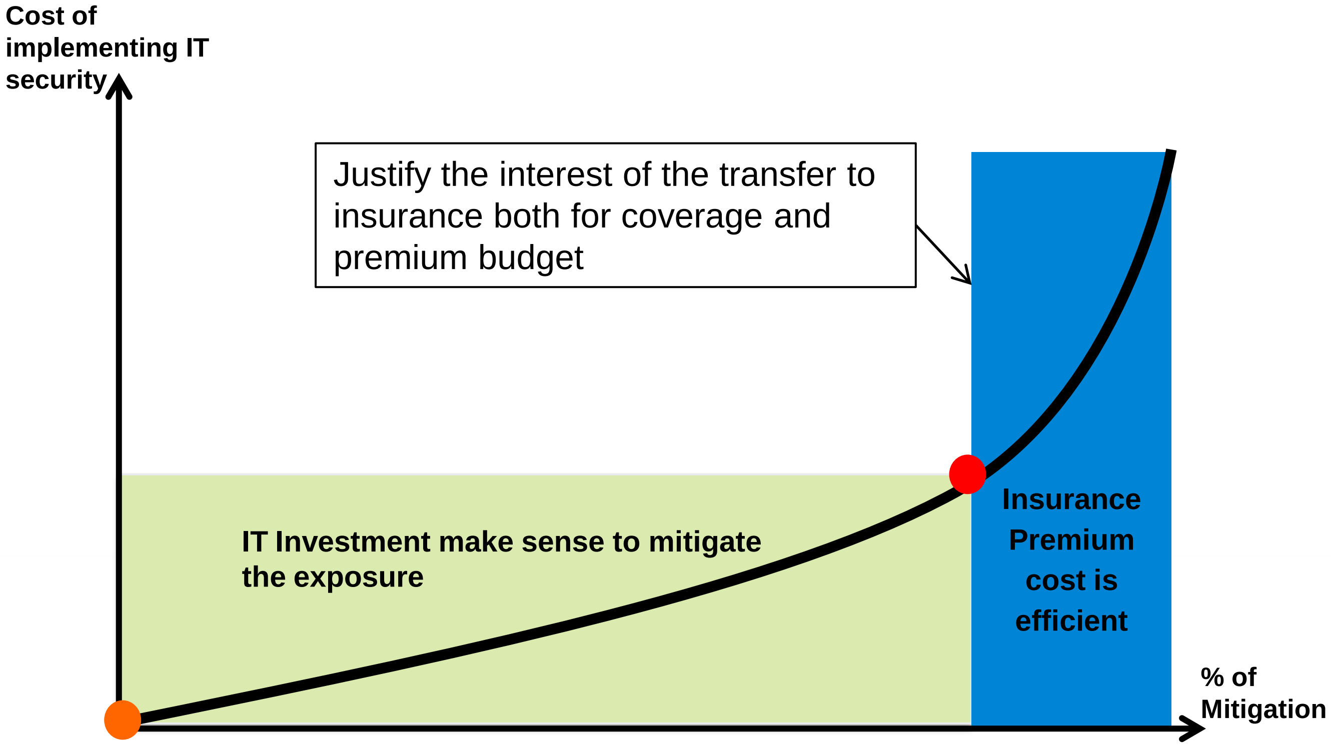
S4: Nulla facilisi. Nunc justo tellus, aliquet eu scelerisque vel, aliquet at ipsum.

S5: Nulla facilisi. Nunc justo tellus, aliquet eu scelerisque vel, aliquet at ipsum.

S6: Nulla facilisi. Nunc justo tellus, aliquet eu scelerisque vel, aliquet at ipsum.

Next Steps
Provide a rationale for mitigation strategy





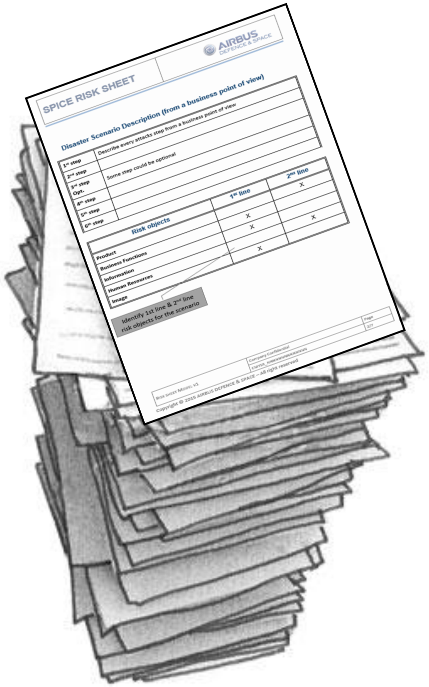
Justify the interest of the transfer to insurance both for coverage and premium budget

- IT investment to reduce the probability of occurrence, until the point of time when costs are too high.
- At that point of time insurance becomes complementary (and not competitive) to IT measures and is efficient from a costs point of view

Challenges

The process needs to be performed regularly and be as exhaustive as possible

- a strategy allowing to manage the roll out of this process across the entire organisation, products and countries
- an efficient process manageable with the operationals



SPICE RISK SHEET

AIRBUS
DEFENCE & SPACE

Disaster Scenario Description (from a business point of view)

1st step	Describe every attacks step from a business point of view
2nd step	Some step could be optional
3rd step Opt.	
4th step	
5th step	
6th step	

Risk objects	1st line	2nd line
Product	X	X
Business Functions	X	
Information		
Human Resources	X	X
Image		

Identify 1st line & 2nd line risk objects for the scenario

Page 2/7

Company Confidential
CMYSR_NNNNNNNNNNNNN

Risk sheet Model V1

Copyright © 2015 AIRBUS DEFENCE & SPACE – All right reserved

Conclusion

- Business Impact Analysis on Cyber Risk analysis is complex and requires sensibilisation from the operational management
- This is a useful tool to identify the key assets that could be a potential targets
- Scenario identification and quantification help to rationalise future effort on cybersecurity and is an helpful tool to dialog with top management
- Proper cyber risk management is a key asset for the companies in their discussion with customers, suppliers, and rating agencies
- Regulation is evolving and is heading towards an obligation to communicate for each company on this topic