1 Workshop 1

1.1 Scope and security baseline

1.1.1 Missions

Protect the confidentiality of exchanges.

1.1.2 Participants

Director (decision maker) and vice-director who is in charge of the IT service.

1.1.3 Timeframe

Everything happens in one day.

Schedule: 10h: Start 10h10: Recall of the main concepts 11h50: Presentation of the case study 12h10: Starting meeting 12h40: Debriefing meting/Workshop 1 13h00: Lunch break 14h30: Meeting with director/Workshop 2 and 3 16h: Meeting with vice-director/Workshop 4 17h: Risks and counter-measures

1.2 Perimeter

1.2.1 Business values

Business value	Feared event	Impact	Gravity
Factory plans	3., 7., 6.	6.	
Original architectural designs	3., 7., 6.		
3D virtual models	3., 6., 7.		
Brand reputation (remove from BV)	4., 5.		
Integrity of calculations (perimeter is confidentiality, remove)	4., 5.		
(marketshares?)	3., 7.		

Focus on 2 or 3 Business value is the data, not integrity or confidentiality of it Restrict perimeter to confidentiality

1.2.2 Supporting assets

1. IT service (7 computers, 2 laptops, wifi, ethernet, tablets, PAO presentation tool)
2. USB keys where the files are stored
3. Paper documents
4. Expansive design software (ARC +, SIFRA, SPOT)
5. Website

1.3 Feared events

1. k
2. 3.
3. Spyware installed on computers (keep for threat scenario? 4th workshop) IMPACT: Factory plans models and customers private data can be stolen GRAVITY: 3
4. Violation of integrity of calculations, generation of wrong plans IMPACT: Buildings might collapse, some refactoring might be necessary, additional costs and delays GRAVITY: 4
5. Liability issues relative to the manipulation of private data of IMPACT: Fine, lawsuits, negative impact on the brand GRAVITY: 3 clients (be more specific)
6. Robbery due to lack of control system (threat scenario?) IMPACT: Loss of marketshares, fine (stealth of personal data of clients) GRAVITY: 3
7. Loss of marketshares due to spying and lack of confidentiality IMPACT: Decline in revenue GRAVITY: 2

1. Leak of factory plan...
2. Continue with second business value
3. Only one feared event by BV
4.

2 Workshop 2: Risk sources

1. Employee OBJECTIVE: Revenge, sell to the competitors MOTIVATION: +++ RESOURCES: ++ ACTIVITY: + PERTINENCE: Moderate
2. Competitors OBJECTIVE: Steal marketshares, acquire new technologies, improve their image MOTIVATION: +++ RESOURCES: +++ ACTIVITY: +++ PERTINENCE: High
3. Non related hackers OBJECTIVE: Steal asset to sell (data, plans), train, add computers to a botnet MOTIVATION: ++ RESOURCES: ++/+++ ACTIVITY: ++ PERTINENCE: Moderate
4. State spies OBJECTIVE: Acquire new technologies, sabotage, gain information about military buildings MOTIVATION: + RESOURCES: +++ ACTIVITY: + PERTINENCE: Low
5. Ideological hacktivists OBJECTIVE: Leak informations, stop production of military infrastructures MOTIVATION: + RESOURCES: ++ ACTIVITY: ++ PERTINENCE: Low
6. Service providers OBJECTIVE: Sell data MOTIVATION: + RESOURCES: +++ ACTIVITY: + PERTINENCE: Low

Keep 1. and 2.

3 Workshop 3: Strategic scenarios

3.1 Stakeholders

1. Clients DEPENDENCY: 4 PENETRATION: 2 CYBERMATURITY: 1 TRUST: 3
2. Cleaning service DEPENDENCY: 2 PENETRATION: 2 CYBERMATURITY: 1 TRUST: 2
3. Service providers DEPENDENCY: 3 PENETRATION: 3 CYBERMATURITY: 4 TRUST: 4

3.2 Threat scenarios

1. Spyware installed on computers (Competitors send malicious emails) GRAVITY: 3
2. Theft of computers/laptops (Competitor, unrelated robbers) GRAVITY: 3
3. Employee sells secret data about project GRAVITY: 2
4. Network access gained by competitors GRAVITY: 3

3.3 Security measures

1. Encrypt data RESIDUAL THREAT: 0,2
2. Restrict access privileges of employees RESIDUAL THREAT: 0,8
3. Implement physical access regulation (alarms, etc.) RESIDUAL THREAT: 0,5
4. Authentication for network devices RESIDUAL THREAT: 0,5

4 Workshop 4: Operational scenarios

1. Competitor bribes an eager employee and gets access to some confidential data OVERALL LIKELIHOOD:
2. The closet containing the USB drives gets forced open by the cleaning service, hired by the competitors, and the files are disclosed OVERALL LIKELIHOOD:

5 Workshop 5:

Now evaluate in terms of motivations and resources Be selective and keep short perimeter Identify and evaluate stake holders and identify threat scenario Focus today on one or two scenarios

6 Questions for Rémi

1. How to evaluate residual threat?
2. Does it indicate a percentage of what is remaining?

3. What is expected about operational scenarios?
4. Should we put more operational scenarios in the final report?

1. What do they fear? Losing money, contracts (by access to data and technologies)
2. How specific do we need to be about the attacks etc.? As specific as possible (workshop 4)
3. What liability issues might the company have? Problems come from personal data, conversations
4. Keep integrity? No
5. Should we add something in the beginning about norms, GDPR...? no