EASA
European Aviation Safety Agency

Aviation Cybersecurity Roadmap Research needs

Cyrille Rosay
Senior Expert Avionics – Cyber Security
Certification Directorate

Your safety is our mission.

An agency of the European Union

Context

Outcomes of EASA Conference on Cybersecurity in Aviation, 22th of May 2015 in Brussels

- Civil Air Transport System is vulnerable to cyber attacks
  - wide range of possible effects of cyber attack
  - exposing safety of flight,
  - Reducing capacity of European Air Transport,
  - increasing financial operational cost,
  - societal issues like loss of public’s trust in
    - Operators
    - Civil Air Transport

Cyber Security –
An Industry Perspective

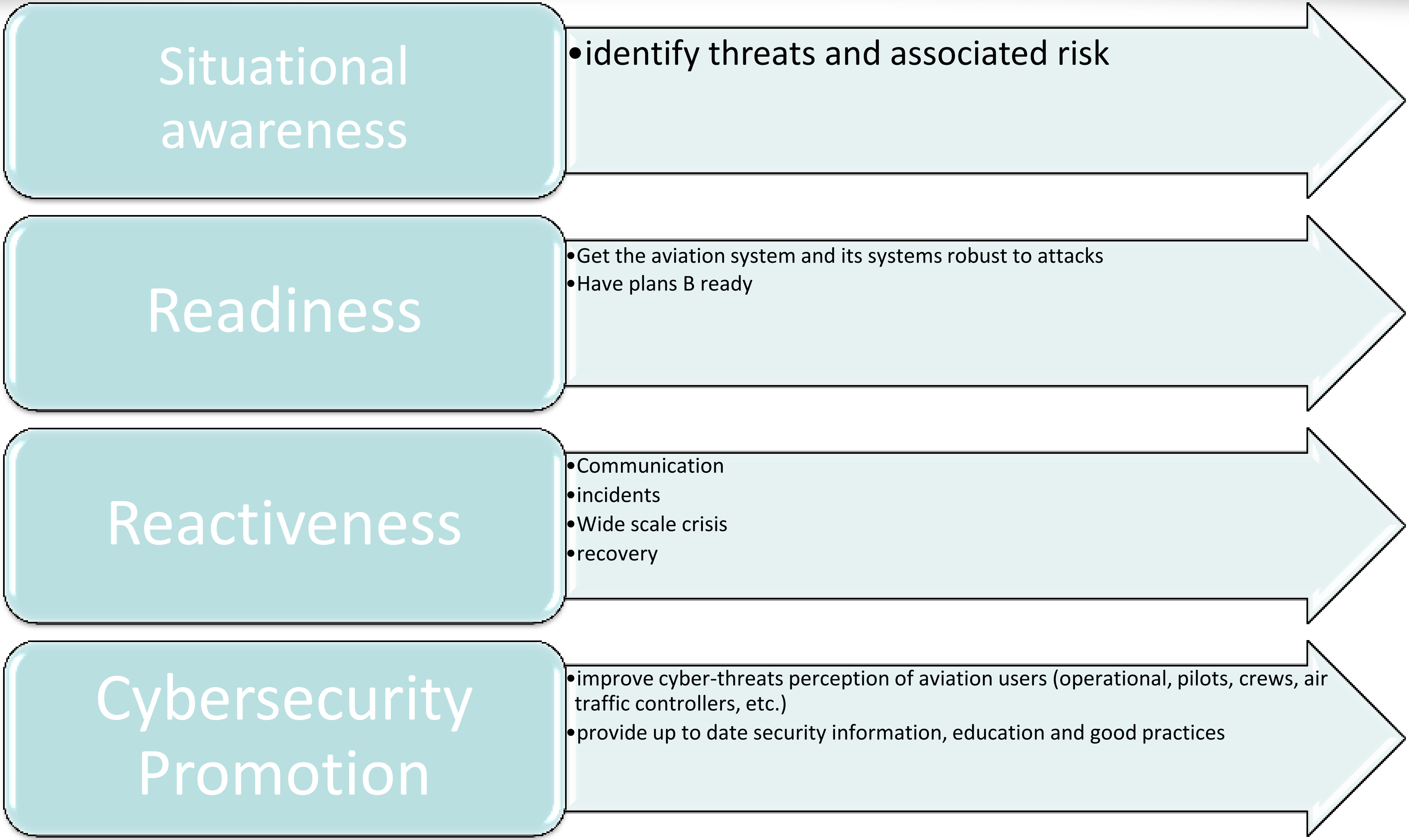
- an actions plan needs to be developed,
  - together with aviation stakeholders
  - EASA focus primarily on European Aviation Safety

EASA roadmap on cybersecurity

- 4 objectives
- 4 enablers

Note: it is a preliminary status, the EASA roadmap on cybersecurity is “work in progress”

Global strategy - Objectives



Situational awareness

- identify threats and associated risk

Readiness

- Get the aviation system and its systems robust to attacks
- Have plans B ready

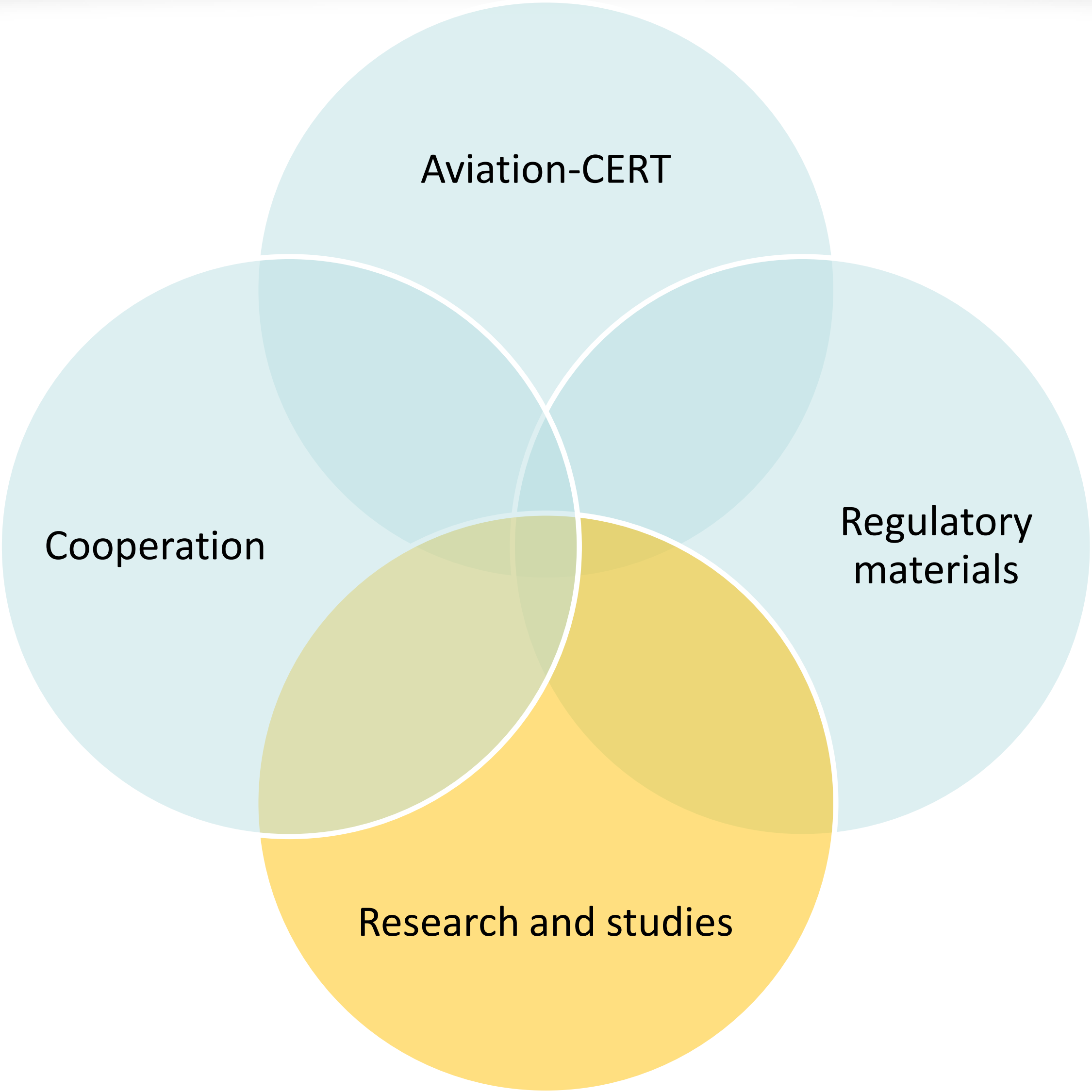
Reactiveness

- Communication
- incidents
- Wide scale crisis
- recovery

Cybersecurity Promotion

- improve cyber-threats perception of aviation users (operational, pilots, crews, air traffic controllers, etc.)
- provide up to date security information, education and good practices

Global strategy / Enablers



Aviation-CERT

Cooperation

Regulatory materials

Research and studies

Global strategy / matching

	Situational Awareness	Readiness	Reactive capability	Promotion
AV-CERT	☒	☒	☒	☒
Regulatory Material		☒		
Research	☒	☒		
Cooperation	☒	☒	☒	☒

Situation awareness

- First step: assess the Risk (impact * likelihood)
- Impact assessment (HIGH, MEDIUM, LOW)
  - Identify scenarios
    - On ATM, Aircraft systems, services, airports…
  - Evaluate the impact
    - In operational condition
    - Using average trained resources
- likelihood or difficulty of attack (HIGH, MEDIUM, LOW)
  - Analysis of architectures
  - Analysis of systems/software
  - penetration testing

Situation awareness

impact

Likelihood (difficulty)

	LOW	MEDIUM	HIGH
HIGH (easy)	🟧	🟥	🟥
MEDIUM (moderate)	🟩	🟧	🟥
LOW (difficult)	🟩	🟩	🟧

- Risk
  - **High** loophole that needs to be quickly secured, and immediate workaround should be identified
  - **Medium** serious security gap identified that would need timely answers. Workarounds have to be ready
  - Low acceptable from a safety point of view, may need long term study.

Readiness

- Objective
  - Get systems robust by design
  - Maintain systems robustness during operation
  - Get the aviation system resilient
    - a.k.a. prepare plans B

- Short-term
  - Study temporary solutions (workaround) for threats with High risk
- Mid-term
  - Study cost and feasibility of improvement for threats with High risk (i.e. design improvement, protocols, security tools…)
  - Study temporary solutions for threats with Medium risk
- Long term
  - Study means to lower Medium risk

Conclusion

- Research is an important enabler of the EASA cyber security roadmap

- 3 research areas:

Risk assessment

Difficulty of attack

Security Controls