Conclusions

1. *Risk management*
2. *Crisis management*
3. *Technology*

Risk Management Needs

1. *Testing and certification is needed not only of components but also of systems and subsystems*
2. *Scenario building and scenario based stress tests*
3. *Holistic mind set and capability to think outside of the box when creating scenarios*
4. *Exercise, exercise, exercise..*
5. *Improve the capability to focus attention on the essential, to avoid waste of resources*
6. *Little exchange among CI operators of good practice on how to prevent cyber attacks*

Crisis Management Needs

1. Communication among relevant parties, both as terminology and as connectivity

2. Forecasting systems, intelligence and maps have proved to improve the ability to act during disasters, so more of them are needed.

3. Cybersecurity maybe ignored during a crisis, this may have important implications

Technology Needs

1. *Physical security*
2. *CCTV*
3. *Detectors*
4. *Cybersecurity good practice*

New technologies are around the corner, although aviation is looking more for simplification. Training of personnel to the new technologies is essential. Financial support to the operators to test new security solutions on site and as part of their systems could stimulate the process of exchange of good practice and standard development. Manufacturers are key to security and more collaboration among operators and the solution providers to improve the products and contribute to the competitiveness of the EU industry.

European Commission

erncip

Thank you for your attention!

Much more information on the ERNCIP website at

http://ipsc.jrc.ec.europa.eu/?id=688

INNOVATION UNION

EUROPE 2020

JRC