

# Cybersecurity is about brand protection

Pascal Buchner

Director ITS & CIO

24 January 2019

**Caspian**  
week







# Agenda

## 5 safety principles

- Segmentation
- Prevention
- Resilience
- Risk management
- Information sharing

## 4 recommendations

- Strategy
- Risk management
- Risk assessment
- Threat intelligence

## Conclusion

380,000

Payment cards  
compromised



**IOActive**

Satcom  
vulnerability

Cyber threats  
are very visible  
in the medias

The industry response  
can be improved

- Education
- Transparency
- Integration

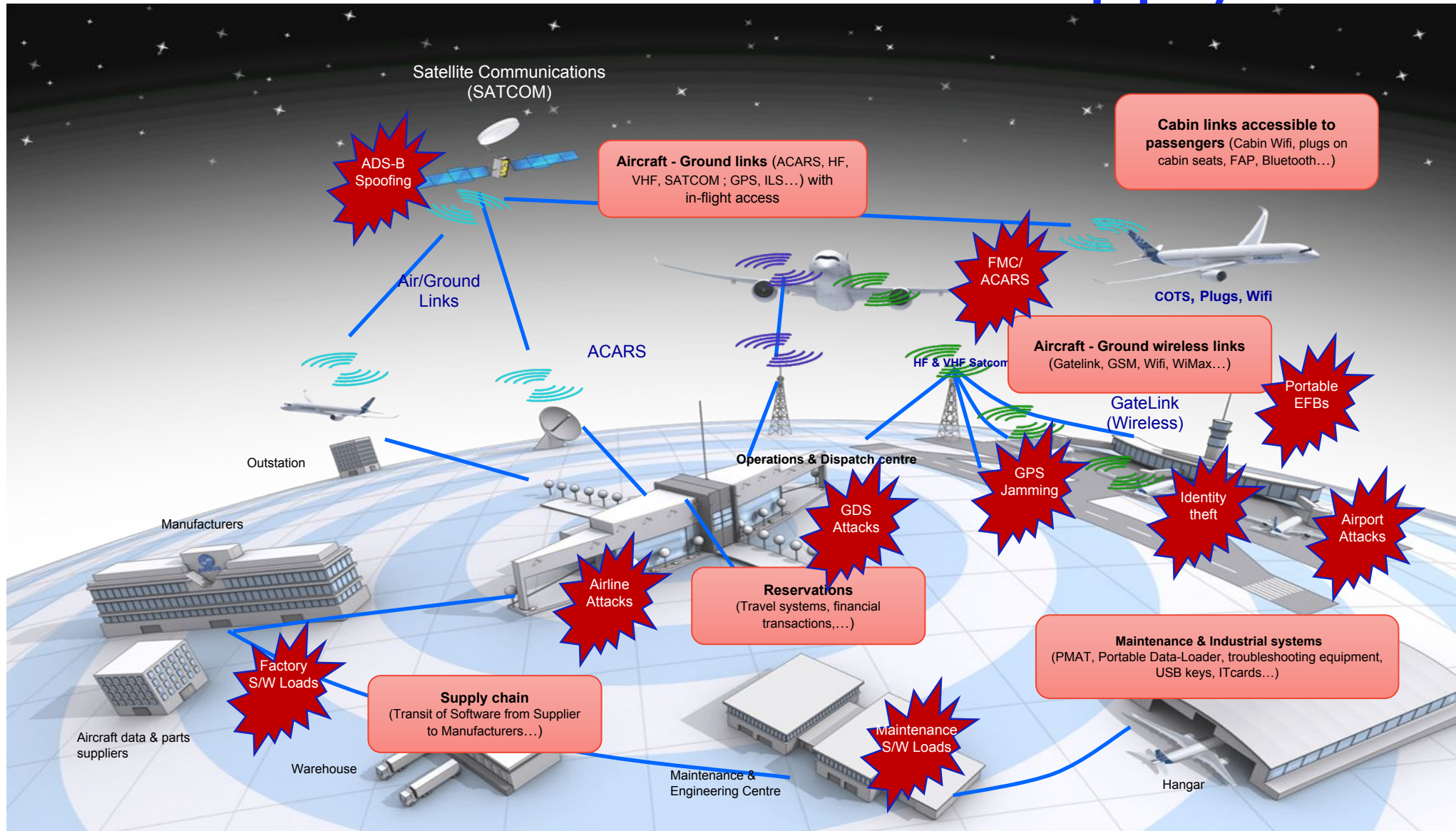


9m

Passenger  
personal  
information stolen



# Threats are across the entire supply chain







# Problem statement

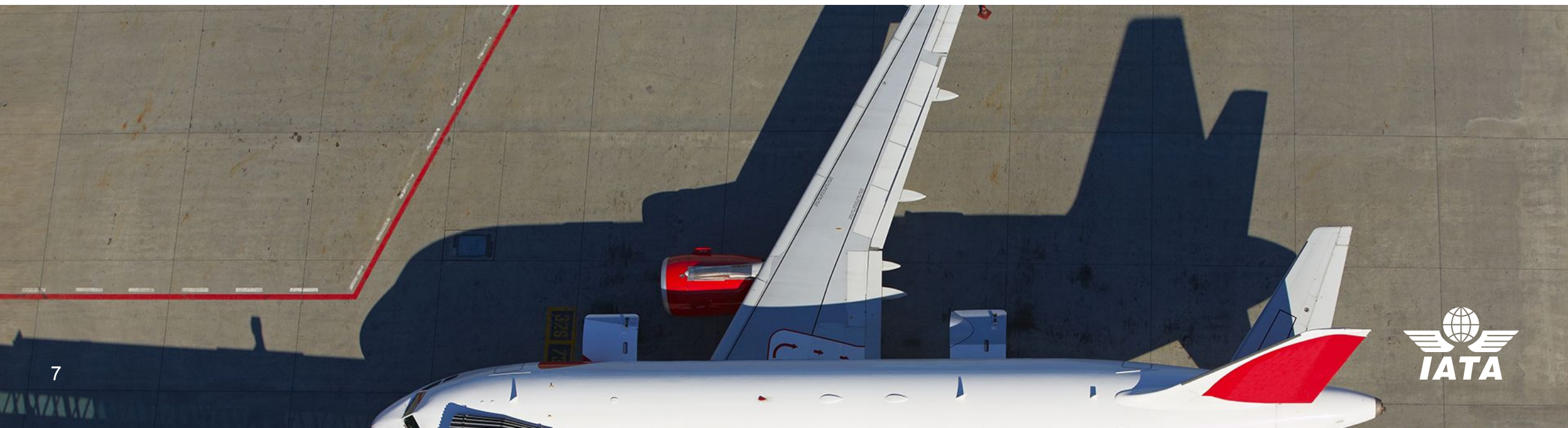
“how do we secure resilient customer trust in our organization?” which is more than just securing technology. It’s a multi-discipline effort including the entire aviation sector

it’s also about being able to demonstrate, communicate and reassure your customers that they are right to trust you.



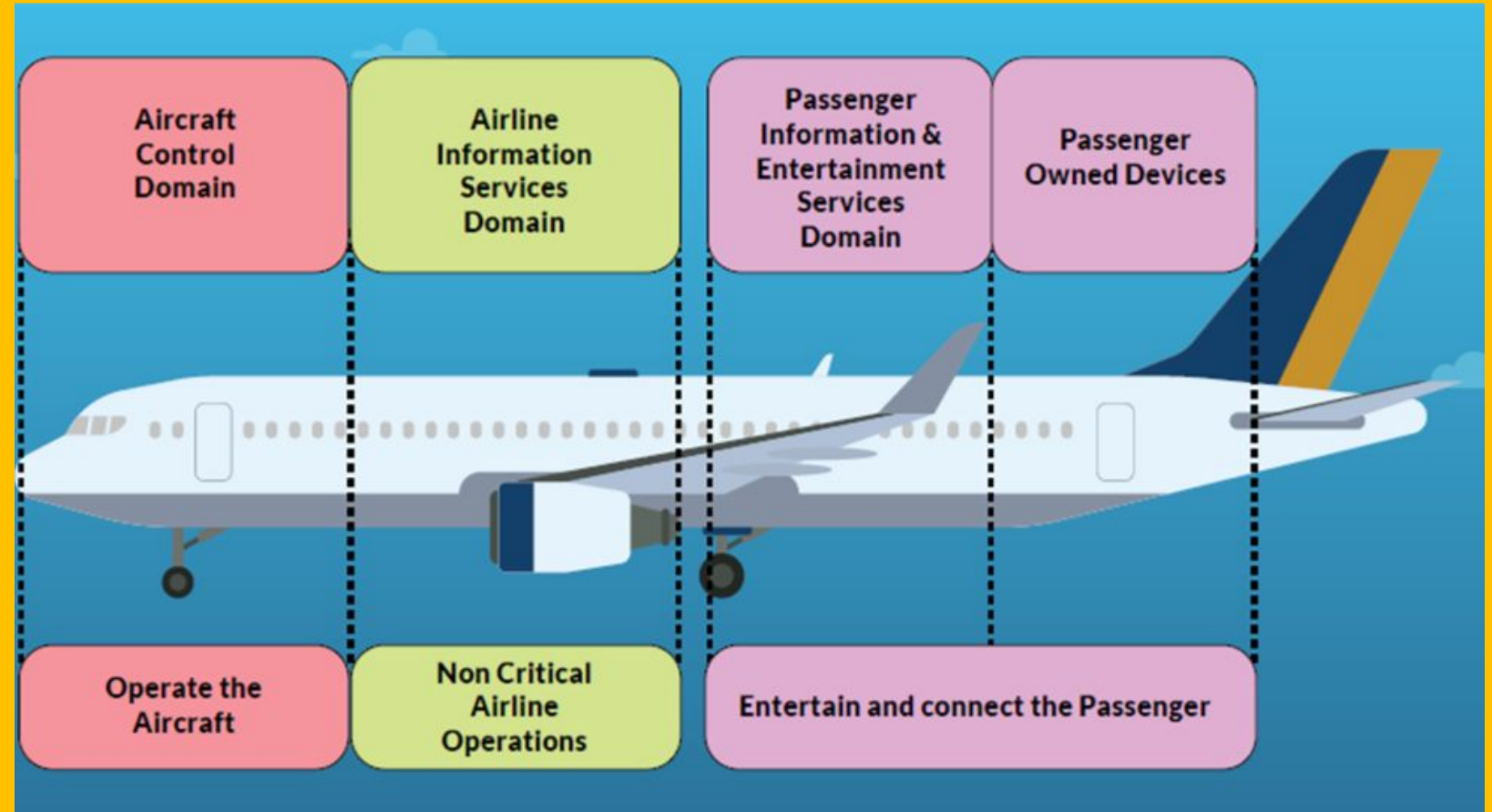


# 5 aircraft safety principles



# 1. Critical network isolation

Aircraft safety critical networks are required to be **isolated** in order to avoid forms of avionic domain data corruption;





## 2. Prevention

The **connected aircraft** forms part of the Internet of Things (**IoT**) attack surface







### 3. Resilience by design

Aviation systems must be **demonstrably resilient**, so that in the event of an unforeseen attack, for example, compromising system segregation, it does not cause a critical failure or loss of consumer confidence;



## 4. Risk management

Moving forwards, an **integrated risk management** approach to safety and security, which incorporates a pro-active assessment of hazards, vulnerabilities and threats is required to ensure information security risks are managed within acceptable levels.





## 5. Information sharing

To best minimize systemic cyber risk quickly, responsible disclosure of vulnerabilities, cyber threats and risks and **information sharing must be encouraged** and supported internationally.



# 4 Recommendations



1. Develop a cyber security strategy recognizing that security measures to mitigate information security risks include physical and organizational perspectives



2. Promote the development of an Integrated Risk Management approach (SeMS and SMS) to manage cyber risk to aircrafts



3. Encourage Industry stakeholders to share threat information in a practical and timely manner



4. Encourage responsible disclosure and sharing of aviation cyber threats, vulnerabilities and risks.



We have the vision of a global cybersecurity framework covering the entire supply chain with an integrated risk management combined with threat intelligence and real time sharing.



# Thank you

Pascal Buchner

[Buchnerp@iata.org](mailto:Buchnerp@iata.org)

[www.iata.org](http://www.iata.org)

