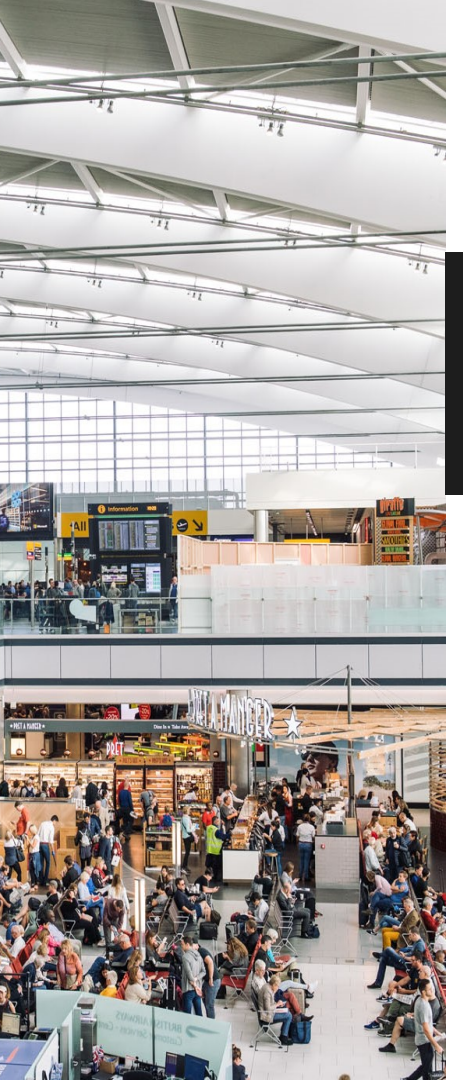
Heathrow

Pragmatic Cybersecurity

Richard Dempers
Eugene Kramer

ADSA24
06.10.2021



Detection / Preventative methods are not 100% effective
Do they create attack vectors?

Problem:

- Threat to security is increasing due to nature of increasingly connected world
- Increasing cases of targeted attempts to compromise security systems, both physical and digital
- Classic IT vs OT vs IIoT- cybersecurity traditionally viewed from an IT perspective
- Detection / Preventative methods are not 100% effective, do they create attack vectors?
- Is Cybersecurity seen as the ‘Business Prevention Department’ ?

Solution:

- Authorities & Regulators developing and implementing new legislation - enforce improved cybersecurity practices
- Airports need to interpret & implement legislation appropriately
- Legislation provides guidance for improvement - responsibility is on airports to go above and beyond the baseline
- IT and OT are equally important - holistic approach
- Cybersecurity encompasses both technology, physical assets and boundaries
- Appropriate risk based approach must be enforced
- Attacks and threats dealt with by defence in depth - multiple layers to defeat attempted breaches

Results:

- Organisations have a clearer understanding of their landscape
  - Landscape is not traditional IT but airports require an understanding of all assets requiring protection
- Understanding the landscape enables a more effective and appropriate set of event triggers and controls
- Correct application of legislative approach and common metrics enables assessment of relative cybersecurity strengths and weaknesses from a regulatory or government perspective

Heathrow

Cybersecurity guidelines – an example

Through our work with Open Architecture and in collaboration we have provided guidelines for cybersecurity best practice
https://www.aci-europe.org/downloads/resources/Open%20Architecture%20for%20Airport%20Security%20Systems_1st%20Edition.pdf
We have assessed the posture of the OEMs and this is leading to a significant change across the industry

Secure the System (Identify vulnerabilities, Manage vulnerabilities, Secure configurations)

1. Audit and Accountability
2. Protected Sensitive Screening Algorithms
3. Configuration Management
4. System and Information Integrity
5. Security Assurance Scanning/Testing
6. Cyber Intelligence
7. Supported Systems

Secure System Access (Secure accounts and privileged users, strengthen and secure passwords, Logging)

1. Access Control (A)
2. Access Control (B)
3. Password Control
4. Identification and Authentication

Secure the Hardware (Secure physical ports)

1. Physical and Environment Protection
2. Personnel Security

Secure the Network (Separate the network, Encrypt the network, Restrict network services)

1. Data at Rest Encryption
2. Systems and Communications Protections
3. Supply Chain Management
4. Vendor Cybersecurity culture
5. Incident Response

Cybersecurity - reference examples

CAP1753: CAA Cyber security oversight process for aviation
CAP1849: Cyber Security Critical Systems Scoping Guidance (caa.co.uk)
CAP1850: Cyber Assessment Framework (CAF) for Aviation (caa.co.uk)
Cybersecurity Framework | NIST