LAM·LHA

SECURITY INNOVATION

VIOLENT EXTREMISM AND INSIDER THREAT IN AVIATION

3 December 2019, WINS

Past cases

- Theft and illegal activities remain a challenge for aviation, but …
- Insider Threat programs focus on Violent Extremism leading to terrorist action against the airport or the aircraft

2011 – Employee in BA IT Department

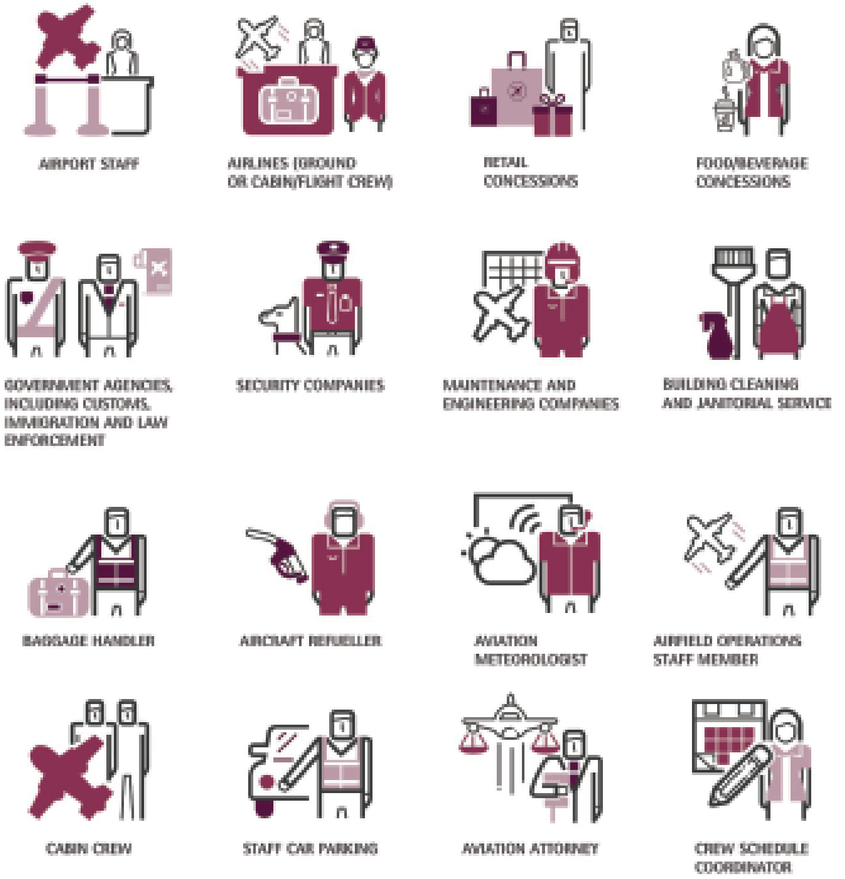
2015 – Metrojet in SSH
Mechanic suspected to have planted a bomb

2016 – Daallo flight
2 airport workers helped smuggle a laptop bomb

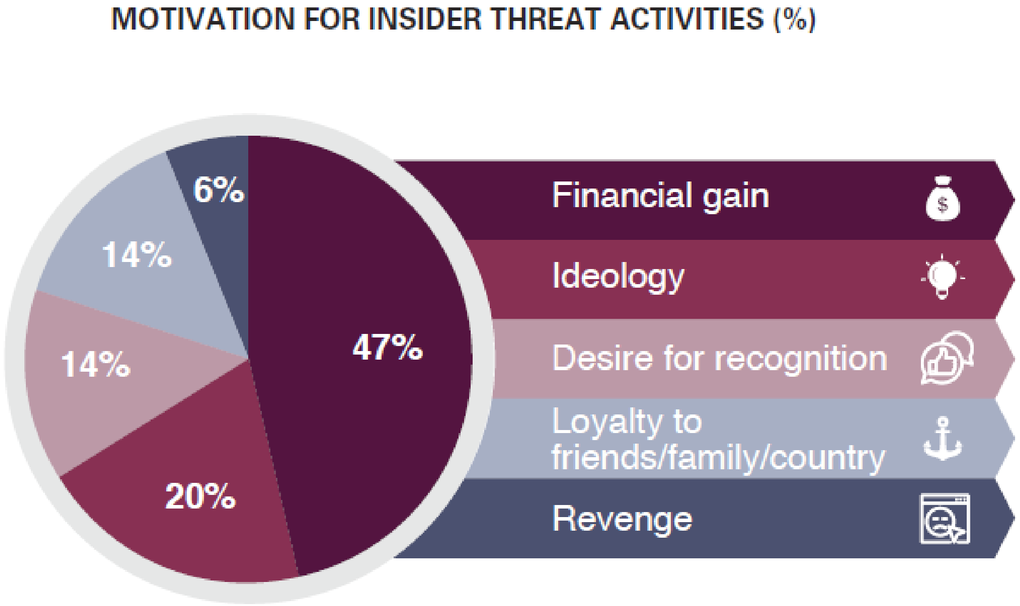
Definitions

Insider : One or more individuals with access, and/or insider knowledge that allows them to exploit vulnerabilities in the transportation domain.

Who can be an insider in aviation?



Motivations and Tactics



- Sabotage
- Terrorism
- Espionage
- Workplace violence

Legal Requirements

- Standards developed by UN institution – International Civil Aviation Organization (ICAO)
- Annex 17 to the Chicago Convention – focus on Aviation Security – applicable to all 191 ICAO Member States
  - Definition of restricted zones requiring control for authorized access: ID verification before entry into Security Restricted Area (SRA) of the airport
  - Staff screening and unpredictability
  - Supervision of movements within SRA to prevent unauthorized access to aircraft
  - Pre-employment and recurrent background checks for staff having unescorted access to SRA

Insider Security Programs

- Program models :
  - Specific insider security program (cross-departmental)
  - Integration in company policies (HR / Legal / IT)
  - Integration in company security program (integrated in security audits)

- Governance :
  - Internal : Centralized oversight or delegated to each division – need for cross-departmental coordination
  - External : Coordination committee . Map your stakeholders and your risk – law enforcement, suppliers, third-party contractors, etc .

Key Measures

Pre-Employment

Training

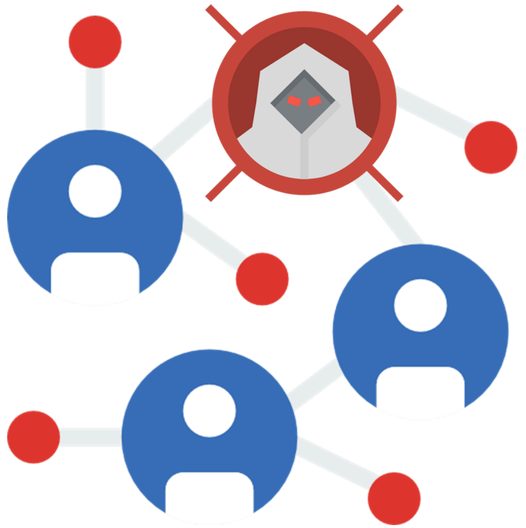
Access Control

Investigation

Reporting

Continuous Monitoring

Post-Employment



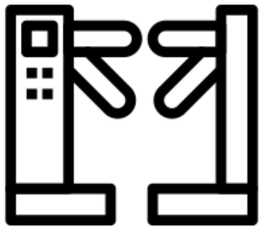
Pre-Employment & Training

- Differentiate measures depending on sensitivity of position
- Training of HR team on how to read a CV and to do the interviews
- Pre-employment checks / background checks
- Company charter

- Integrate information on insider threat in awareness training
- Recurrent training / exercises
- General behavior detection training for recruitment teams and managers

Access Control & Continuous Monitoring

- Risk assessment on different areas of infrastructure and IT systems
- Limit access to specific zones through badging
- Security features of staff ID (use of biometrics / reconciliation with work schedule)
- Screening of person and items carried upon entry
- Unpredictability of inspections / upon entry and in premises
- Behavior-based detection: on premises and in systems (access logs)



Reporting and Investigation

- Reporting tools – depends on company's culture / consider feedback – not just for employees, but also third parties
- Validate reported information
- Cooperation with law enforcement

Sanctions and Exit measures

- Importance of clear company policies to avoid conflicts with employment laws
- Clear disciplinary process – possibility to re-position person temporarily during investigation
- Importance of exit interviews / measures: access badges / codes removed

LAM·LHA

SECURITY INNOVATION

+32474980398

MCLAURENT@LAM-LHA.COM

LAM-LHA.COM