Insider Threat Awareness

Mr. Robert McLaughlin
TSA Representative
North Africa &
Middle East

Global Ministerial
Aviation Summit
Riyadh, Saudi Arabia
August 30, 2016

Transportation
Security
Administration

Overview

Discuss the key elements of insider risk and how to mitigate the unique security risks associated with those with privileged access.

Insider Risk Headlines

Explosion Causes Cabin Rupture on Flight from Somalia

The detonation of an IED smuggled onto Daallo flight 159 by possible airport workers, illustrates the wild card still facing global aviation despite years of efforts to combat terrorism: the inside threat.

Feb 2016

Atlanta Airport Baggage Handler Jailed for Smuggling Guns

A Delta Airlines baggage handler was jailed after being caught by police for smuggling 18 firearms through an employee-only access point onto a flight to New York.

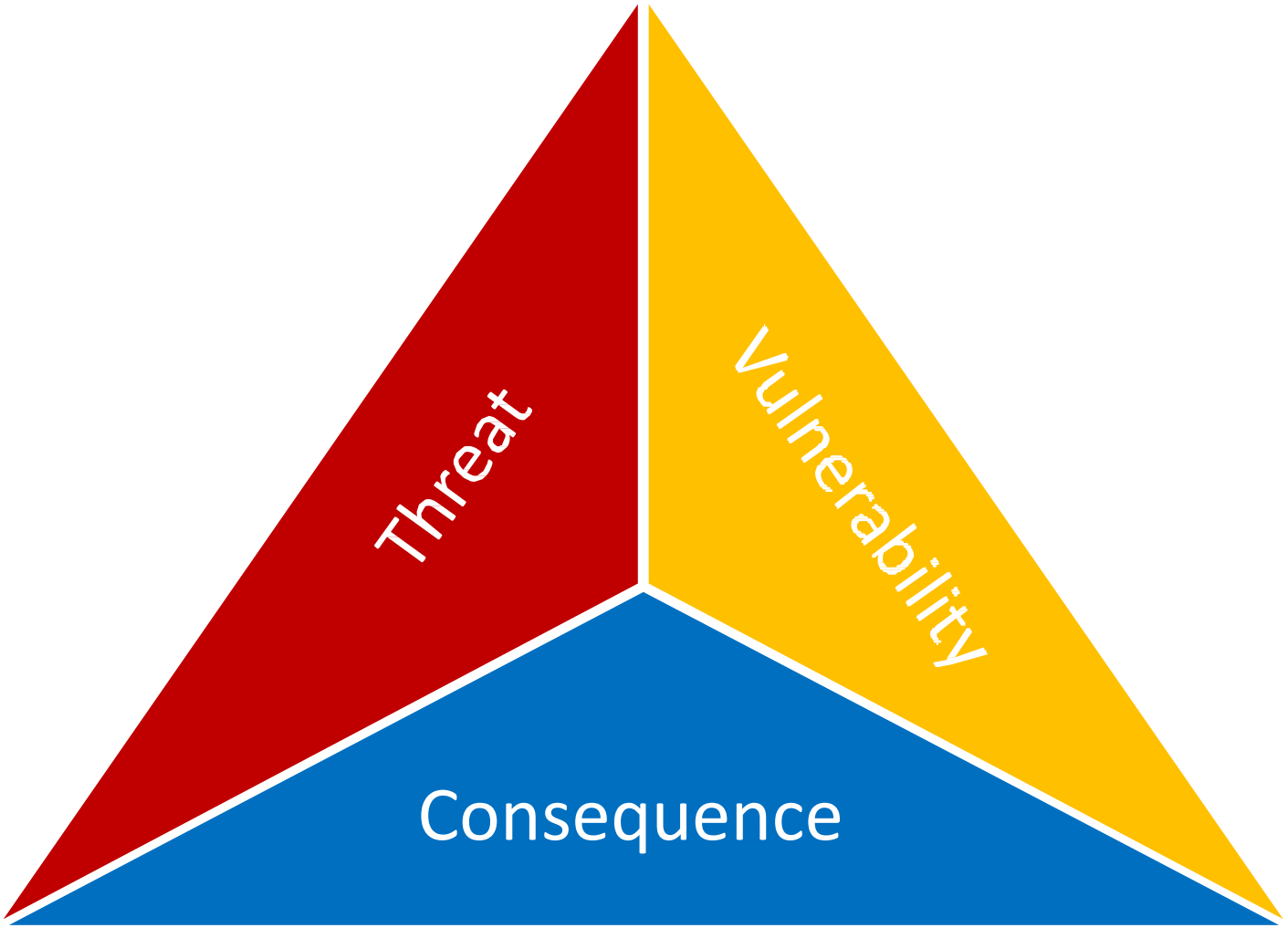
Dec 2014

The Terrorist inside British Airways

A former British Airways worker has been convicted of four counts of preparing acts of terrorism.

Feb 2011

Insider Risk



Insider Risk

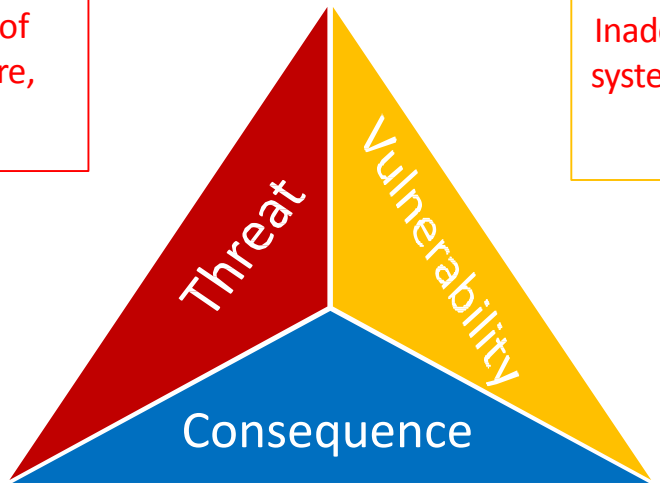
Risk = Threat * Vulnerability * Consequence

Threat

Unique access to secure areas of the airport, critical infrastructure, and sensitive information

Vulnerability

Inadequacies and/or characteristics of a system/asset that could permit an act of unlawful interference



Consequence

The outcome of an act of unlawful interference, in human, economic, political, and reputational terms under a reasonable worst-case scenario

Insider Definition

Working Definition:

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

Who is an Insider?

- Airport support staff
- Airport management and administration
- Contract security staff
- Airport vendors
- Flight crews
- Airline ticketing agents
- Aircraft Mechanics
- Baggage Handlers
- Contract aircraft custodial crews
- Catering staff
- Law Enforcement
- Customs Agents
- Security Screening Personnel
- Air Traffic Controllers
- Fixed Base Operators
- Former employees

Drivers of Insider Risk

Ignorance

Lack of awareness of policies and procedures creates risk

Employees being uninformed of polices and procedures is a challenge, particularly when dealing with emerging threats as well as new employees

Complacency

Lax approach to policies, procedures, and potential security risks

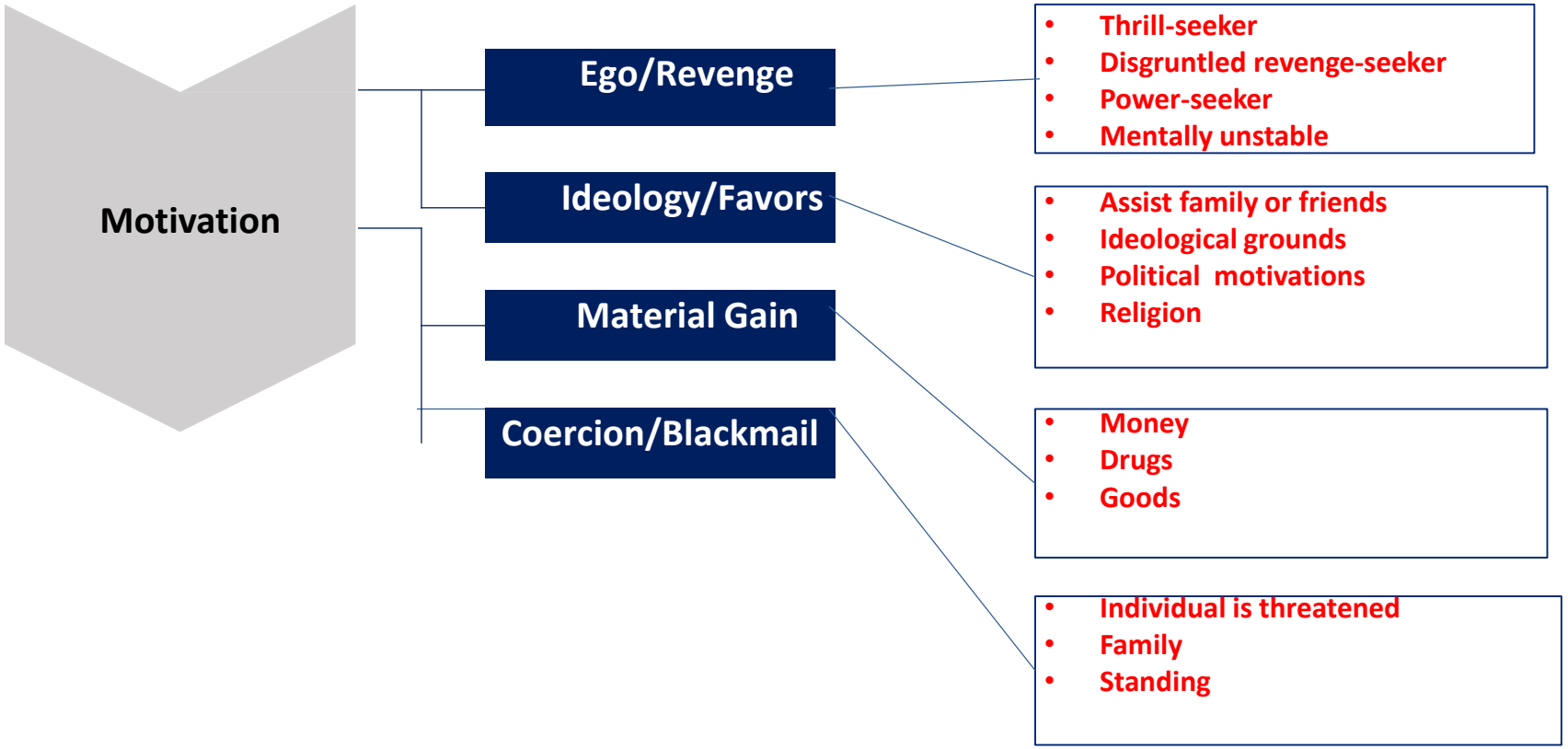
Violators often assume that their specific behavior doesn't have a noticeable impact or that no one is monitoring their behavior

Malice

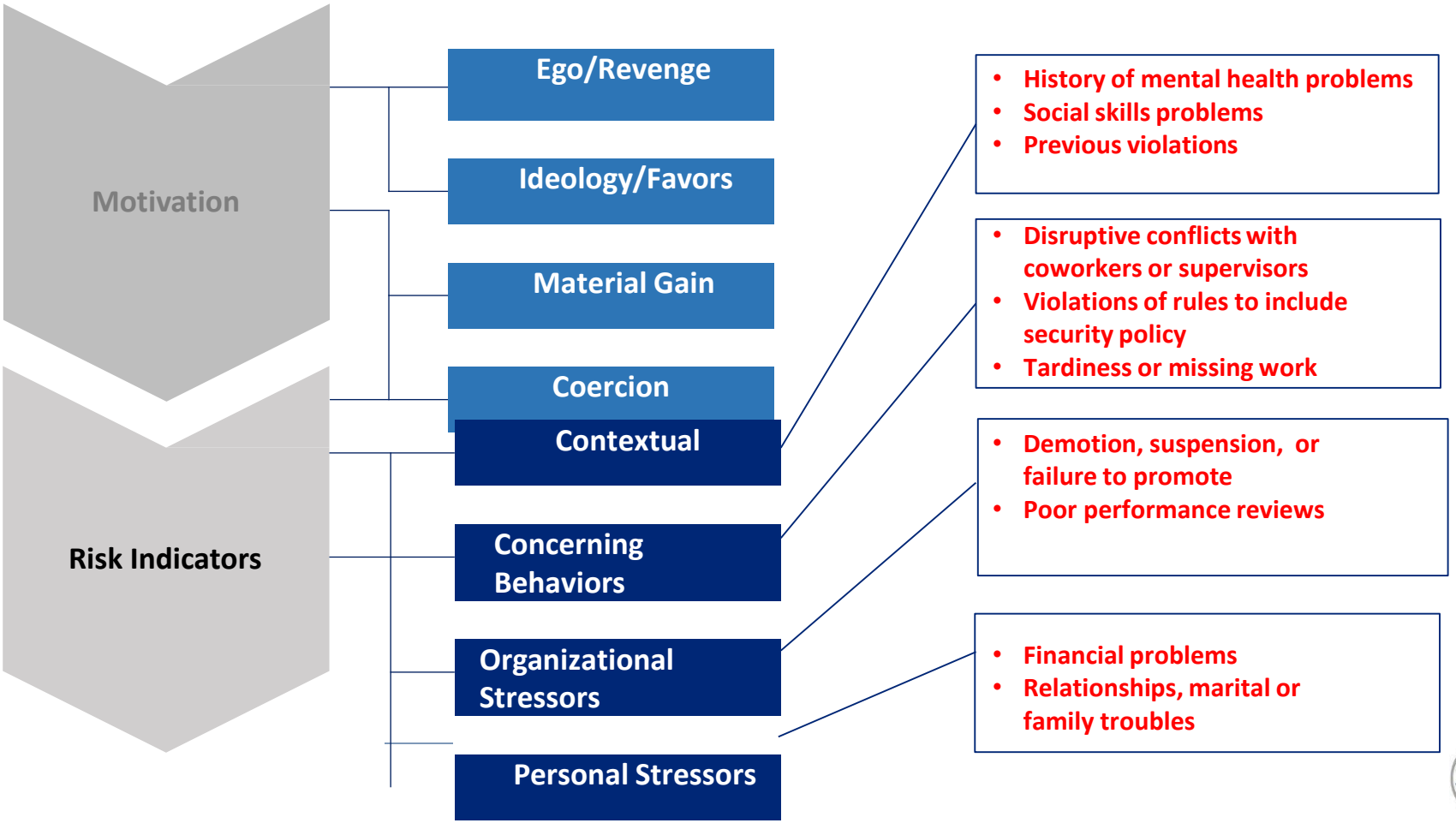
An act that is malicious and intentional in nature to cause damage

Insiders typically develop a plan in advance that someone within the organization may detect

Malicious Insider Motivations



Behavioral Risk Indicators



Insider Tactics

Espionage

Use of insider access to obtain sensitive information for exploitation that impacts national security

Terrorism

Use of access to commit or facilitate an act of violence as a means of disruption or coercion for political purposes

Security Compromise

Use of access to override or circumvent security controls (e.g. drug and contraband smuggling)

Physical Property Theft

Use of insider access to steal material items (e.g., theft of passenger possessions or equipment)

Sabotage

Intentional destruction of equipment or material

Information/Intellectual Property Theft

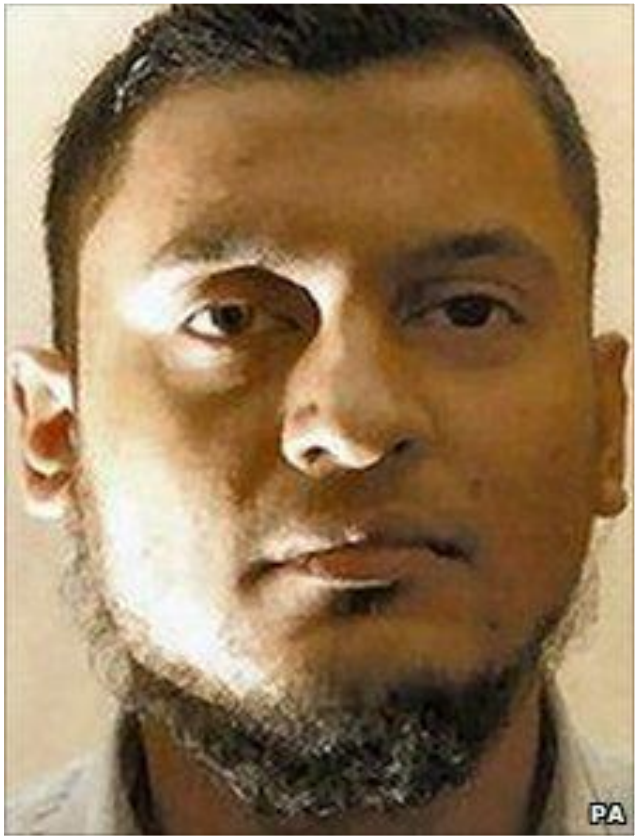
Use of insider access to steal or exploit information

Workplace Violence

Use of violence or threats that causes a risk to the health & safety of the workforce & traveling public

Malicious Insider: Rajib Karim

- February 2011
- Worked as British Airways (BA) employee
- Offered Foreign Terrorist Organizations help with disrupting and damaging airline computer systems
- Used his knowledge of BA databases and airline procedures as the basis for his recruitment
- Identified 2 BA employees as possible recruits for terrorist activities



Malicious Insider: Terry Loewen

- December 2013, attempted to bomb the Wichita Airport
- Radicalized via internet/Al Qaeda in the Arabian Peninsula
  - *Inspire*
- Used SIDA badge to bypass security
- Brought materials through checkpoint
- Studied the airport layout, flight patterns, and passenger volume
- Court documents revealed outwardly expressed interest in anti-American activities including supporting violent jihad

Example: Terry Loewen

Personal Factors – Motivation

Ideology/Identification

Behavioral Indicators

Suspicious foreign contact
Anti-American statements
Previous disregard for policy (weapons violation in 2009)

Insider Countermeasures

Security controls, people, processes, physical attributes, and/or technology in place to deter, detect, prevent, and/or abate an act of unlawful interference, i.e. reduce vulnerabilities.

People, process, and/or technology that assist in mitigating Insider risk i.e. reduce vulnerabilities.

Countermeasures and Insider Risk

Solution

Insiders have trusted and verified positions that give them access to secure areas, therefore insider specific countermeasures are required.

Ignorance, Complacency, and Malice can be countered with tools, policies, and unpredictable countermeasures targeted towards insiders.

Insider Countermeasures

- Employee Lifecycle Management
- Access Controls
- Training and Awareness
- Policies and Procedures

Employee Lifecycle Management

- ✓ Hiring Criteria: qualifications and requirements for each position
- ✓ Vetting: criminal history and employment background checks for permanent and temporary employees
- ✓ Recurring vetting: background checks at periodic intervals throughout the employee's tenure

Access Controls

- ✓ Access Control Systems:
  - Airport guards, proximity cards, biometrics, PIN codes, lock & key, stop lists, vehicle identification
- ✓ Terminal Access Points
  - Baggage belt doors, sterile area boarding, gates, employee screening checkpoint, fire/emergency doors, operational/maintenance doors
- ✓ Airside Access Points:
  - Emergency crash gate, pedestrian and vehicle entrances

Access Controls, Cont'd.

- ✓ Personnel Identification Systems: identify level of authorized access
- ✓ Screening: daily physical inspection of employees, their vehicles and belongings
  - Physical search/pat down
  - X-ray screening
  - Canine
  - Behavioral detection
  - Metal detectors
  - Advanced Imaging Technology (AIT)
  - Explosive Trace Detection (ETD)

Training and Awareness

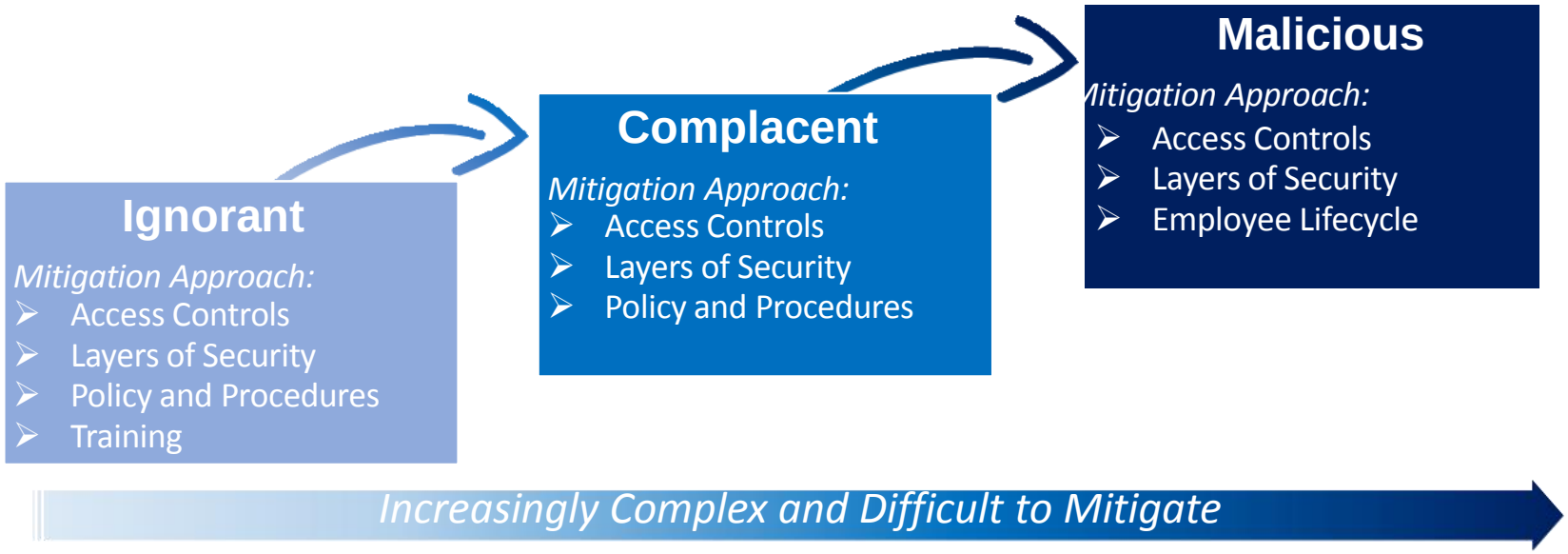
- ✓ Training: initial and ongoing insider risk training for all those with access
- ✓ Behavioral Indicators: employees recognize and report warning signs
- ✓ Monitoring: anomalous behavior detection and video surveillance (CCTV)
- ✓ Reporting: programs should encourage employee participation in mitigating insider risk, provide anonymous reporting options, and clearly identify methods to notify supervisors, airport operations staff, and security of suspicious activity

Policies and Procedures

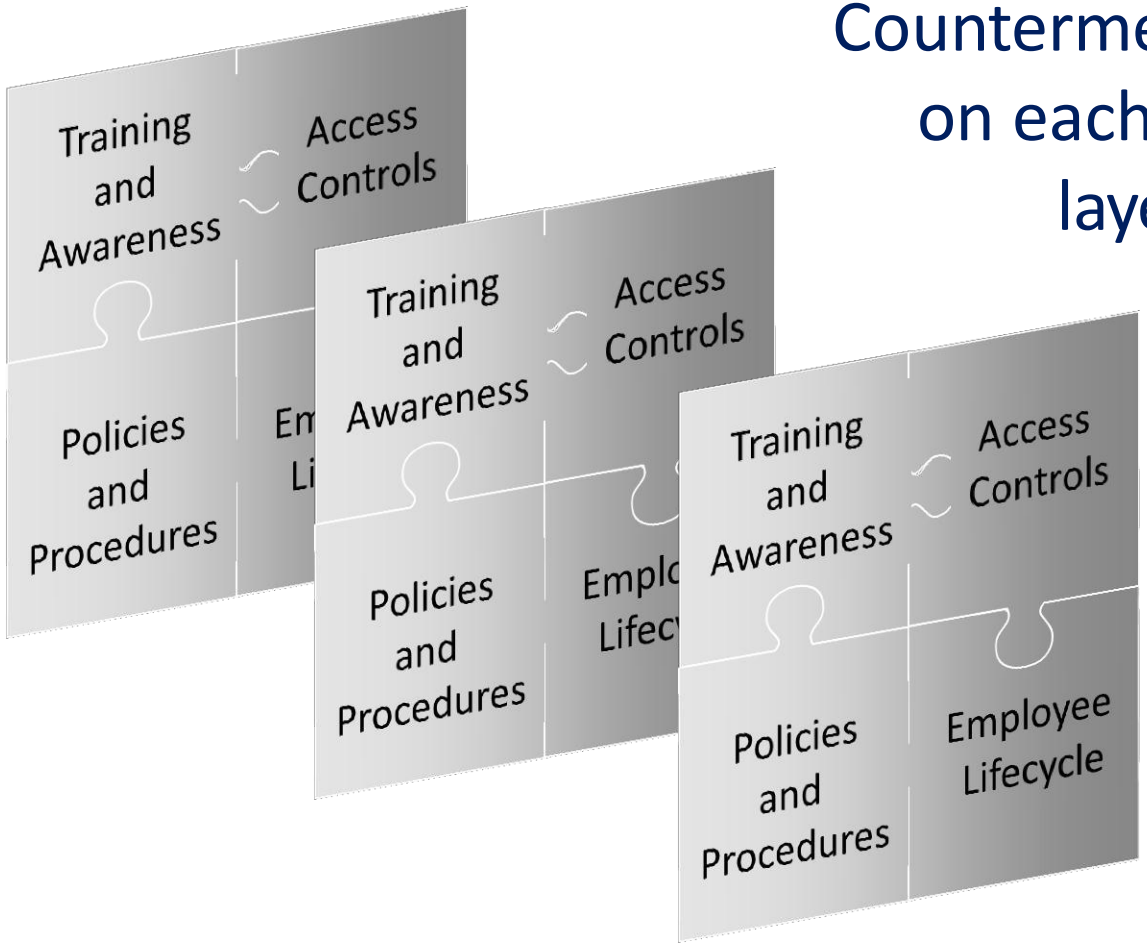
- ✓ Require personnel display ID at all times while in the security restricted area
- ✓ Maintain strict control and accounting system for access badges
- ✓ Establish employee termination procedures
- ✓ Ensure separation of duties (dividing functions so people do not complete duties alone)
- ✓ Least privilege (access only what is necessary for the job)
- ✓ Include unpredictability in deployment of countermeasures
- ✓ Document and consistently enforce policies and controls

Layered Approach to Mitigating Risk

Mitigation approaches are additive and form a layered approach to reducing risk. In addition, all mitigation approaches include unpredictable deployment of countermeasures.



Layers of Security



Countermeasures can build on each other to form a layered approach to reducing risk

Mitigating Insider Vulnerabilities

Recognize the Vulnerabilities

- Where are the security gaps?
- How effectively are you mitigating the threat with currently deployed resources?
- What programs are in place to ensure you have a Secure Workforce?
- How effective is your vetting process in reducing the risk of granting access to the wrong people?
- Do employees comply with access policies and procedures?

Identify Countermeasures

- Can existing countermeasures be modified or enhanced?
- Do you need to implement new countermeasures?
- What will make more effective countermeasures?
- What current static countermeasures can be made unpredictable?

Questions