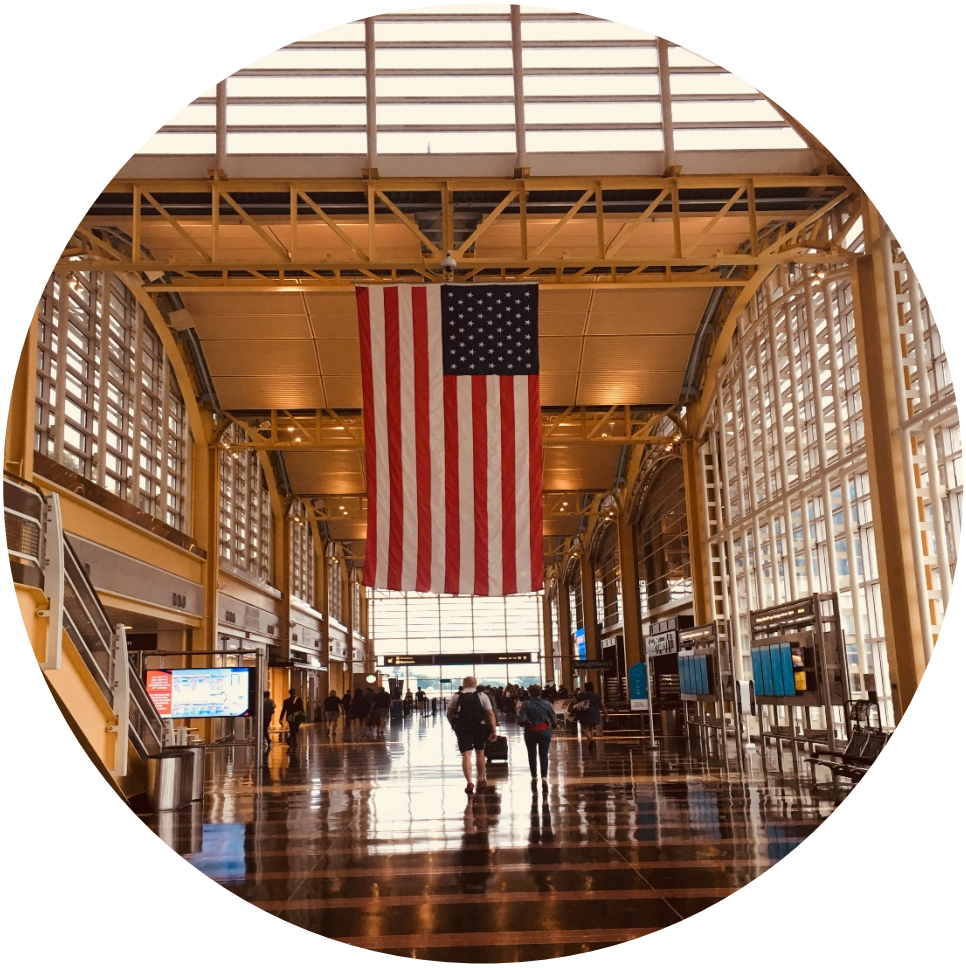
Deloitte.



Aviation Insider Threat Mitigation

Considerations and Recommendations

November 2020

Top 10 Considerations

The aviation industry faces a variety of insider threats that have the potential to adversely impact the public and the industry itself. Aviation, specifically airports, are highly complex environments, both from an operational perspective and a governance perspective – which creates challenges in mitigating insider threats. This challenge is compounded when an organization has not incorporated insider threats into the risk mitigation strategy. A string of recent, high profile cases – including the theft of a commercial passenger plane from Seattle-Tacoma International Airport in 2018, and a 2019 incident during which an aircraft mechanic at Miami International Airport used his access to sabotage an avionics component onboard an aircraft -- demonstrate how insiders can use their knowledge and access to perform malicious activities.[1]

These cases highlight vulnerabilities and a common misperception of adequate processes that would prevent, detect and respond to insider incidents. To prepare for, and ultimately prevent such incidents, aviation leaders can augment existing security procedures through the development of a holistic insider threat program. The ten considerations below offer insights into how aviation leaders can take tactical actions to develop their own insider threat capabilities; they are informed by the design, build, and implementation of insider threat programs across the public and private sector including the aviation industry.

1. Define the insider threat

Few organizations have a specific internal working definition for insider threat since security and IT budgets have historically prioritized external threats. An insider can be an employee, a contractor, or a vendor that commits a malicious, complacent or ignorant act using their trusted and verified access. Defining the threats specific to the airport ecosystem is a critical first step to formulating a program that will inform the program's size, structure, scope, and implementation.

2. Define the risk tolerance

Define the critical assets (e.g. facilities, aircraft, operations, customer information) that must be protected and the organization's tolerance for loss or damage in those areas. Identify key threats and vulnerabilities in your business and in the way you do business. Tailor the development of the insider threat program to address these specific needs, the organization's risk tolerance, and the threat types posed. The key is to balance security with business/operational objectives.

3. Engage a broad set of stakeholders

The program should have one owner with input from a broad set of invested stakeholders from across the airport's ecosystem. Establish a cross-disciplinary insider threat working group or community that can serve as change agents and ensure the proper level of buy-in across stakeholders (e.g., airlines, government agencies, third party vendors, and unions). The working group should assist in addressing common concerns (e.g., privacy and legal) and support the development of messaging to executives, managers and the broader airport employee population.

4. Technology alone won't solve the problem

The insider threat challenge is not purely technical, but rather a people-centric problem that requires a holistic and people-centric solution. The program should avoid the common pitfall of focusing on a technical solution as the silver bullet. An insider threat mitigation program should include key business processes (e.g., removal of employee access if disqualifying crime discovered), technical and non-technical controls (e.g., policies), organizational change management components, and security training programs needed to promote an environment of security awareness and deterrence.

5. Trust but verify

Establish routine and random auditing of physical and logical privileged functions. Optimize the effectiveness of vetting programs and consider aperiodic vetting practices. Aviation organizations should trust their workforce but balance that trust with verification to avoid instances of unfettered access and single points of failure. This auditing is particularly essential in areas that are defined as critical.

6. Look for precursors

The FBI's Insider Threat Program recommends behavioral-based techniques to identify insider threats, such as identifying a baseline for how insiders operate (e.g. move around the airport, on and off the network), to then identify anomalies. Insider threats are seldom impulsive acts. Rather, insiders move on a continuum from idea to the insider acct displaying potential risk indicators. These observable behaviors (e.g., failed access attempts, policy violations, and undue access) can serve as potential risk indicators for proactive risk detection.

7. Connect the dots

By correlating potential risk indicators captured in virtual and non-virtual arenas, aviation organizations can gain insights into anomalous behaviors that require human review. This can be achieved using analytic tools that score risky behaviors and help the program connect the dots on emerging threats. This can in turn be used to proactively identify insider threat leads for investigative purposes. It can also shed new light on processes and policies that are either missing or could be improved.

8. Stay a step ahead

Insiders' methods, tactics, and attempts to cover their tracks constantly evolve, which means that the insider threat program should continuously evolve, as well. This is achieved through a feedback mechanism that analyzes the efficacy of potential risk indicators and learnings from prior cases leading to continuous alignment with the changing threat environment. As the bad guys learn and adapt, so does the program.

9. Set behavioral expectations

Define the behavioral expectations of your workforce through clear and consistently enforced policies (e.g., social media, reporting incidents, employee screening, etc.) that define acceptable behavior. Develop strong communication campaigns so aviation community members know what is expected and institute consequences for violating policies.

10. One size does not fit all

Training content should be informed by the level of physical access, privilege rights and job responsibilities. Train the workforce to the specific insider threat risks, challenges, and responsibilities for each position (e.g., baggage handler and flight attendant curriculums should vary). Embed training in onboarding processes and throughout the year.

[1] "Aviation Security: TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals", United States Government Accountability Office, February 2020.

A Path Forward

The COVID pandemic is a seismic shift. It is causing the ground to move beneath nearly every organization. In such difficult circumstances, the resilience of workers is shining through as organizations continue to operate as best they can. However, we are all human, and as the crisis drags on, uncertainty, new technologies, and changing circumstances can introduce risk even to the best prepared organizations. While aviation leaders do not necessarily need to implement all 10 consideration at once, timely steps to address risks and gaps in existing vetting, validation, and employee monitoring processes[2] can save significant disruption and loss of critical assets tomorrow, all while supporting the resilience of the workforce today.

At a time when accountability is a primary leadership responsibility, an insider threat mitigation program bolsters deterrence and provides a mechanism for prevention, thereby protecting the traveling public, the workforce, information, equipment, and facilities. Deloitte[3] takes a proactive, holistic and risk-based approach to insider threat program development, with broad participation required (e.g., airport operators and regulators, airlines, third party vendors, etc.) with support and sponsorship by executive leadership. Deloitte's approach is informed by the development of over three dozen insider threat programs for organizations across a diverse range of industries, including the aviation sector.

For more information, please contact:

Mike Gelles
Managing Director
Deloitte Consulting LLP
mgelles@deloitte.com
+1 202 251 9615

Borna Emami
Senior Manager
Deloitte Consulting LLP
bemami@deloitte.com
+1 202 957 3165

Liz Krimmel
Senior Manager
Deloitte Consulting LLP
ekrimmel@deloitte.com
+1 202 230 4251

Elizabeth Burns
Manager
Deloitte Consulting LLP
eliburns@deloitte.com
+1 571 733 8967

Mark Freedman
Senior Consultant
Deloitte Consulting LLP
mfreedman@deloitte.com
+1 202 207 6097

[2] "Insider Threats to Aviation Security: Airline and Airport Perspectives", Transportation and Protective Security Subcommittee, U.S. Congress, September 27, 2018.

[3] As used in this document, "Deloitte" means Deloitte Consulting LLP, which provides Consulting Services; Deloitte & Touche LLP, which provides Audit and Enterprise Risk Services, and Deloitte Financial Advisory Services LLP which provides Financial Advisory Services. These entities are separate subsidiaries of Deloitte LLP. Deloitte Consulting LLP will be responsible for the services and the other subsidiaries may act as affiliates. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Deloitte.