THE ENEMY WITHIN

Techniques to Combat Insider Threats: Lessons From the Aviation Industry
ASIS VOLUNTEER ROLES
ASIS Strategic Planning Committee
Chairman, Information Technology Security Council
PRESENTER

Richard L. Duncan, CPP.
Assistant General Manager, Public Safety and Security
HARTSFIELD JACKSON ATLANTA INTERNATIONAL AIRPORT
richard.duncan@atl.com
(404) 382-2101
www.atl.com

INDUSTRY VOLUNTEER ROLES
Immediate Past Chairman, Airport Council International
World Standing Security Committee
Past Chairman, ASIS Atlanta Chapter
PRESENTATION

Donald R. Zoufal, CPP., ICAO AVSEC PM, J.D., M.A. Homeland Security, M.A. Public Administration

SDI PRESENCE, LLC
dzoufal@sdipresence.com
www.sdipresence.com

Lecturer,
University of Chicago
dzoufal@uchicago.edu

Delivering Intelligent Technology™
Josh Jackson.

RIGHTCROWD SOFTWARE
josh.jackson@rightcrowd.com
www.rightcrowd.com

INDUSTRY VOLUNTEER ROLES
Vice Chairman, Physical Security Interoperability Alliance, (PSIA)
AGENDA

• Introduction to Enterprise Security Risk Management
  Bates

• Atlanta Airport – Case Study
  Duncan

• Industry-wide Approach
  Zoufal

• Continuous Workforce Assurance as an ESRM Enabler
  Jackson

• Q&A Session
  Panel & Attendees
THE ENEMY WITHIN

Techniques to Combat Insider Threats:
Volume 1—Enterprise Security Risk Management
WHAT IS ENTERPRISE SECURITY RISK MANAGEMENT (ESRM)?

• A management process used to effectively manage security risks, both proactively and reactively across an enterprise
  • quantifies threats, establishes mitigation plans, identifies risk acceptance practices, manages incidents, and guides risk owners in developing remediation efforts
  • Continual assessment of the full scope of security related risks to an organization, and within the enterprise’s complete portfolio of assets
E V O L U T I O N  O F  E S R M

• First Industry Alliance ASIS, ISACA, ISSA – 2005
• CSO Roundtable Definition - January 2015
• ASIS “Global Strategic Priority” - November 2016
• Two year Commission – 2017 (Knowledge Expansion)

Goals:
• More systematic integration into collateral
• Better identification and management
• ASIS Members more effective security professionals

Benefits
• More empowered membership
• Safer Enterprises
• More cost-effective security
ENTERPRISE SECURITY RISK MANAGEMENT PROCESS

1. Identify and Quantify the Enterprise’s Assets

2. Identify and Quantify Security Risks to Each Asset


4. Develop Risk Treatment Plans

5. Continuous Improvement

Intelligence Gathering

Reassess Security Risks

Root Cause Analysis & Post Mortem
BUSINESS VIEW OF ESRM

• Sees security as an **enabler of business**
• Risk owners make **more effective decisions** about risk
• For Security: **enablement**
  • **Trusted advisor** status is cumulative
• Deliver an effective range of **security related services** for customers
• Utilize **security related expertise** already provided from regulatory compliance and ESRM
  • Delivery of **tangentially connected services** for fraud and other business aspects
OPERATIONAL FRAMEWORK FOR ESRM

• An Operations Center to handle enterprise risk events
• Multiple categories of services
• Content provision includes
  • active attention to safety and security
  • customer experience
  • regulatory compliance
  • risk management to optimize bottom line
  • maintain reputation of business and customers
ESRM V. ERM – WHAT’S THE DIFFERENCE?

ESRM

• Uses risk management principles to manage security related risks across the enterprise
• Does not define an organizational structure

ERM

• Uses risk management principles to address enterprise risk issues
• Often defines an organizational structure
• Security Dept may be represented within an ERM program, but ESRM is the process under which security manages security-related risks
TRANSFORMATION

- **Who owns** the risk?
- **Where does ESRM start and end**
- **Management** of all security risks
  - Risk principles
  - Autonomy
  - Transparency
- **Organization**
  - Analyze desired capabilities
  - Define Risk based business skillsets
  - Buying into the transformation
  - Trusted advisors to business
    - Responsibilities
- **Transition from Silos** to Consultants to the Business
  - Ensures risks are elevated to the appropriate level in the organization
SOURCES

- **ASIS Commitment**
  - [https://www.asisonline.org/About-ASIS/Who-We-Are/Whats-New/Pages/ASIS-Makes-ESRM-a-Global-Strategic-Priority.aspx](https://www.asisonline.org/About-ASIS/Who-We-Are/Whats-New/Pages/ASIS-Makes-ESRM-a-Global-Strategic-Priority.aspx)

- **CSO Roundtable Definition**
  - Available from ASIS CSO Center

- **ESRM Commission**
  - Strategy, Collateral & Artifacts coming

- **Annual Seminar Workshop**
  - ESRM 2 part exercise
  - Led by Jeff Slotnick today (Monday)
THE ENEMY WITHIN

Techniques to Combat Insider Threats:
Volume 2—Hartsfield Jackson Atlanta International Airport Case Study
COMPONENTS – VOLUME 2

- Airport Overview
- Airport Operators’ Responsibilities
- Public Safety and Security Priorities
- Evolving Threats
- Insider Threat Description
- Major Threats to Aviation
- Impact to Organization
- Mitigation Strategies
- Questions and Answers
AIRPORT OVERVIEW

- Total passengers in 2016 – 104 million+
  - *World’s busiest airport (19th consecutive year)*

- 6.8 million-square-foot terminal complex
  - *3,700-acre campus*

- 63,000 workers on-site
  - *Employee direct access points*
# AIRPORT OVERVIEW

## Economic Impact

<table>
<thead>
<tr>
<th>SECTOR</th>
<th>JOBS</th>
<th>REVENUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct</td>
<td>245,536 (includes 63,000 on-site)</td>
<td>$35 billion</td>
</tr>
<tr>
<td>Indirect</td>
<td>99,011</td>
<td>$15 billion</td>
</tr>
<tr>
<td>Induced</td>
<td>104,149</td>
<td>$14 billion</td>
</tr>
<tr>
<td>Total</td>
<td>448,696</td>
<td>$64 billion</td>
</tr>
</tbody>
</table>
AIRPORT OPERATORS’ RESPONSIBILITIES

Providing for the safety and security of person and property on an aircraft operating in the transportation system against an act of:

• Criminal violence
• Aircraft piracy
• Introduction of an unauthorized weapon, explosive or incendiary device (TSR 1542.101)
PUBLIC SAFETY AND SECURITY PRIORITIES

- Protect life and property
- Minimize exposure to risk
- Ensure ease of movement
- Facilitate continuity of operations
EVOLVING THREATS

- Knives and guns
- Metallic explosives
- Plastic explosives
- Aircraft
- Vehicular born explosive devices
- Terminal attacks (active shooters)
- Suicide bombers
- Insider threat
INSIDER THREAT DESCRIPTION

Insider threats are individuals with authorized access to information or organizational assets that allows them to exploit vulnerabilities or systems, either intentionally or unintentionally, to inflict harm or damage to the organization or others.

An insider threat could be employees, contractors or vendors with access at any level of the organization.
MAJOR THREATS TO AVIATION

- Failing to comply with policies, procedures or regulations
- Committing theft of goods or services
- Committing acts of violence
- Committing acts of smuggling
- Committing acts of sabotage
- Committing acts of hijacking
- Allowing others to commit criminal or terrorist acts against airport, airlines or other entities
IMPACT TO ORGANIZATION

- Denial of service
- Negative press
- Lack of confidence
- Loss in revenue
- Weakened brand
MITIGATION STRATEGIES

- Intelligence and Information Sharing Program
MITIGATION STRATEGIES

- Intelligence and Information Sharing Program
- Employee Vetting
MITIGATION STRATEGIES

- Intelligence and Information Sharing Program
- Employee Vetting
- Security Awareness Training
MITIGATION STRATEGIES

 Intelligence and Information Sharing Program
 Employee Vetting
 Security Awareness Training
 Identity Management System
MITIGATION STRATEGIES

- Intelligence and Information Sharing Program
- Employee Vetting
- Security Awareness Training
- Identity Management System
- Access Control
MITIGATION STRATEGIES

- Intelligence and Information Sharing Program
- Employee Vetting
- Security Awareness Training
- Identity Management System
- Access Control
- Surveillance System
MITIGATION STRATEGIES

- Intelligence and Information Sharing Program
- Employee Vetting
- Security Awareness Training
- Identity Management System
- Access Control
- Surveillance System
- Compliance and Enforcement
MITIGATION STRATEGIES

- Intelligence and Information Sharing Program
- Employee Vetting
- Security Awareness Training
- Identity Management System
- Access Control
- Surveillance System
- Compliance and Enforcement
- Random or Full Inspections
MITIGATION STRATEGIES

- Intelligence and Information Sharing Program
- Employee Vetting
- Security Awareness Training
- Identity Management System
- Access Control
- Surveillance System
- Compliance and Enforcement
- Random or Full Inspections
- Random or Full Employee Screening
OTHER MITIGATION STRATEGIES

- Automatic badge deactivation
- Reduce badge expirations
- Badge activity audits
- Random inspections throughout the Air Operations Area/Secure areas
- Covert operations
THE ENEMY WITHIN

Techniques to Combat Insider Threats:
Volume 3 — Lessons From the Aviation Industry
Numerous differing policies, process and technologies are applied inside and outside the airport.

Typically commercial airports have multiple security levels depending upon activities in any given area.
AIRPORT RISK MANAGEMENT PROCESS

Elements of critical infrastructure
- Physical
- Cyber
- Human

Set goals and objectives
Identify infrastructure
Assess and analyze risks
Implement risk management activities
Measure effectiveness

Information sharing

Source: GAO presentation of NIPP framework | GAO-16-632

AIRPORT RISK MANAGEMENT PROCESS

Regulated Process Under 49 CFR 1542 Including Requirements for

- Employment History Checks
- Criminal History Records Checks
- Verification of Eligibility to Work
- Security Threat Assessment
- Security Training
- Authorized Signatories
- Trusted Agents
- Audit Requirements

### AVIATION’S PARTNERED VETTING ENVIRONMENT

<table>
<thead>
<tr>
<th>Enrollment</th>
<th>Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicant provides biographic and biometric information to airport operator. Airport operator submits information to TSA.</td>
<td>Airport operators responsible for implementing access control system as part of TSA-approved security plan.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Background check</th>
<th>Renewal</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSA vets and adjudicates terrorist and immigration information, and provides results of criminal history checks to airport operator.</td>
<td>In April 2015, TSA modified existing requirements to address the need for recurrent criminal history checks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Issuance</th>
<th>Revocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airport operator issues access badge to employee.</td>
<td>Airport operators can revoke a badge if an individual is no longer employed by airport employer, or if an airport is informed by TSA of derogatory information related to immigration status or during recurring criminal history records or recurring terrorist screening checks.</td>
</tr>
</tbody>
</table>

LINKING TO NEXT GENERATION IDENTIFICATION (NGI)

FBI Next Generation Identification (NGI)

• System to replace IAFIS (the integration system for biometrics and criminal histories)

• AFIS modified to AFIT (more accurate algorithms)

• Facial Recognition

• Iris Pilot

• Latent and Palm Prints

• Rap Back & RISC

INSIDER THREAT TRIAD

- Intentional
- Reckless
- Negligent

Malicious Actors

The Three M’s

Militantly Stupid

Mental Lapsers
THE ENEMY WITHIN

Techniques to Combat Insider Threats:
Volume 4 — Continuous Workforce Assurance as an ESRM Enabler
CWA enforces security through automated interaction with dynamic data sources to allow or deny access based on policies such as:

background checks of the workforce (employees, contractors, tenants)

CWA promotes workforce safety in the areas of:

training, mobilization, (e.g. – security, driving & HAZMAT)

fatigue and time-on-site reporting

CWA ensures that compliance both to policies and regulatory requirements, is continuously enforced providing full audit capabilities to determine the effectiveness of the implemented processes
CWA Security Enforcement

CWA enforces security through automated interaction with dynamic data sources to allow or deny access based on policies such as:

- Background checks of the workforce (i.e. - employees, contractors, tenants)
- Area owner approvals for access requests
- Automated, periodic access reviews
CWA Workforce Safety

CWA promotes workforce safety in the areas of:

Training, (e.g. – security, driving & HAZMAT)

Fatigue and time-on-site reporting

Random Screening
CWA Compliance Assurance

- CWA ensures compliance
- Policies and regulatory requirements are continuously enforced providing full audit capabilities
  - Effective based on the implemented processes
  - Can be used to identify insider threats and anomalous behavior

CWA drives cost reductions and productivity gains
CWA: Return on Investment Experiences

- Access-related tickets: 7,000 per month (3 FTEs)
- $1M USD cost associated with unaccounted for cards
- Higher education hired 5 FTEs at peak times for access allocation

Automate access based on role and location

Self-service approach

70% reduction in tickets. 3 FTEs down to 1

Reduce manpower costs and show where the problems are

Integrate with student system and allocate standard access

Zero FTEs

Self-service

securityexpo.org
CWA: Return on Investment Experiences

- Compliance reporting delays (1 FTE @ 1 week per month)
- Terminated employees still have access
- 29 steps and long training manual using Easy Lobby

- Integrate systems to remove silos. Add workflows to audit activities
- Link to HR/AD Off-boarding
- Guided procedure (9 steps)

- Full compliance 1 click reporting
  Avoid fines
- Immediate removal
  Less disgruntled employee risk
- Better experience for visitors and no on-going training
CWA: Return on Investment Experiences

- 4% of $700M spend estimated in over-invoicing from contractors
- PACS entry/exit data automates contractor reconciliation
- Large percentage of $28M ‘recovered’
- 3 hours to complete a 2,500 person evacuation drill
- Implemented real-time mustering
- Reduction to 20 minutes Huge savings Increase in safety
- Monday morning: 15 FTEs waiting to process temporary cards
- Provide reception with the ability to authenticate and replace cards
- Reduce to 1 FTE and card/access replacement time
THANK YOU!

QUESTIONS AND ANSWERS

securityexpo.org