2019 Curacao Aviation Security Conference

Dan daCosta

SITA Cybersecurity Lead - Americas

Agenda

1. Who is SITA
2. Threat Landscape for Air Transport Industry
3. Top Threats: What are they, and how to defend against them
4. What SITA does to protect itself and it’s customers

Who is SITA

SITA – An Air Transport Industry Leader

- Dedicated to air transport, 100% owned and driven by the community
- We transform air travel through technology – for airlines, airports and aircraft
- Nearly every passenger trip relies on our technology
- SITA supports almost every airline and airport in the world

1,000 Airports – presence

65+ years industry experience

2000+ Strong global service team

200 Countries and territories served

WE CONNECT **13,500** air transport industry sites

2,800 Customers — airlines, airports, services and governments

Threat Landscape

CYBER THREAT LANDSCAPE

Actors

HACKTIVISTS

Information disclosure, disruption, reputation

CRIMINALS

Loyalty Programs, fraud, ransomware...

STATE & COMPANY DESTABILIZATION

Espionage, service disruption, assets destruction

Challenges

TECHNOLOGY

Digital and Smart
Legacy Systems
Inventory and Patching
New cyber weapons

PEOPLE

Human vector
Shortage of expertise

REGULATION

Data Privacy, Aviation Industry, Critical Infrastructures

Business Impacts

- COMPLIANCE
- FINANCIAL
- OPERATIONAL
- REPUTATION

Trends

Inc.

REGISTER FOR THE INC. FAST

The CEO of Delta Air Lines Was Asked What He Worries About Most. His Answer Will Truly Frighten Customers

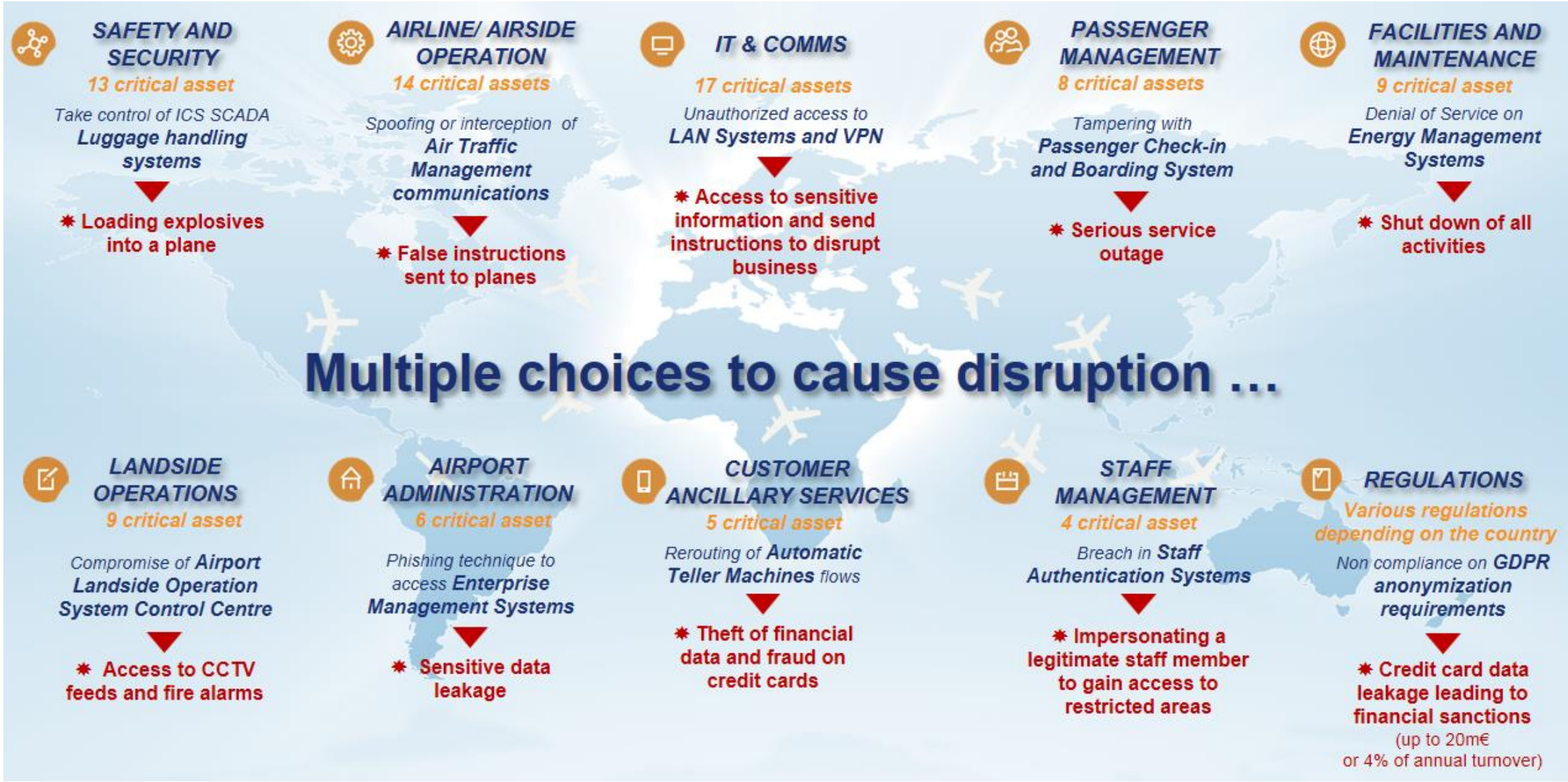
Never imagine an airline CEO is worried about the things you're worried about.

By Chris Matyszczyk *Owner, Howard Raucous LLC* @ChrisMatyszczyk

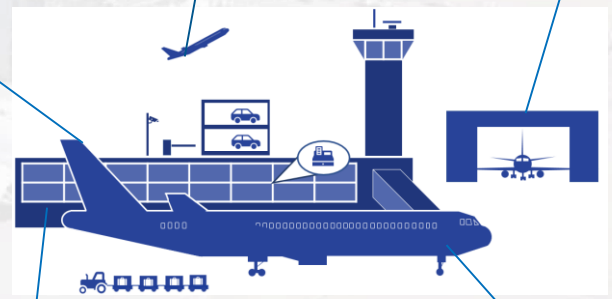
https://www.inc.com/chris-matyszczyk/ceo-of-delta-air-lines-has-worries-that-will-make-customers-shudder.html

Airports… a complex operating environment

…with many systems and processes



Result: Hackers bombard aviation sector with over 1,000 attacks per month!



*Top of the agenda for CIOs at both airlines and airports, are investments in **cyber security** and cloud services. … both airlines and airports agree that the number one priority for their investments is cyber security.*

… 95% of airlines and 96% of airports – plan to invest in major programs or R&D on cyber security initiatives over the next three years. Source SITA

Top Threats

Top airline cyber attack types

(Based on SITA Research of ATI incidents)

1. **Phishing, Ransomware**
2. **Cloud security risks**
3. **Frequent Flyer, Ticketing Fraud & Scraping via BOTs**
4. **OT / IoT**
5. **DDoS**
6. **Insider threat**
7. **Supply Chain / 3rd party**

Continue

Phishing: Defining the problem

- Phishing is sending emails to trick recipients into divulging information, opening a file, or clicking on a link. It is called “fishing” due to the similarity of using a bait in an attempt to catch a victim. It is believed nearly 80% of attacks start with phishing.
- Examples:
  - Many, search Internet
- Aviation Business Impact:
  - Data Leakage, Malware Infiltration, Ransomware, PII Customer/Employees Data Breach, Information Leakage, Regulatory Implications/Penalties, Reputational Damage, Spyware
- Likelihood factors
  - The more realistic and personalized the Emails, the more effective they are. Airline phishing attack has 90% success rate , Lack of User Awareness, Lack of phishing email assessment capability, Lack of suspicious email reporting capability.

Phishing: Reducing the risk

- **People**: Awareness Training, Internal Phishing Campaign tests
- **Technology**: SPAM filters, Threat Intelligence (Proactively combat phishing campaigns), Web filter to block malicious websites, Solution to scan attachments for malware and viruses, Solution to promptly evaluate phishing emails, Mail Systems integrated with an alert generation mechanism for users to immediately report suspected emails, Reverse Engineering expertise, Browser add-ons and extensions can be enabled on browsers that prevent users from clicking on malicious links, Install an Anti-Phishing Toolbar.
- **Process**: Incident Response, Forensics

Ransomware: Defining the problem

- Ransomware is a type of malicious software from crypto-virology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.
- Examples:
  - Many, search Internet
- Aviation Business Impact:
  - Operations & Business Process Disruption, Ransom (Financial loss), PII Customer/Employees Data Breach, Information Leakage, Regulatory Implications/Penalties, Reputational Damage
- Likelihood factors: Lack of…
  - user awareness, anti-malware, phishing prevention, patching mechanism, incidence response capability, threat intelligence, network visibility (who is on your network), SOC, data backup and restoration procedures

Ransomware: Reducing the risk

- See Phishing recommendations
- **People**: User awareness
- **Technology**: Advance malware protection (Email & Endpoints), Web ransomware protection, Continuous threat intelligence, Network visibility and monitoring, Security Operations Center, Ad-blocking capacities and anti-spam filters
- **Process**: Regular Back-ups and restore rehearsals, Incidence response capability, Ransomware response exercise (Readiness), Patch and configuration management, Network segmentation

Return

Cloud Security Risks: Defining the Problem

- Cloud security risks a risks that come from unsanctioned use of insecure cloud services, or use of any cloud service in an inappropriate way.
- Examples:
  - Many, search Internet, Asian Airline using pdf converter that “owns” data, European Airline employee uploads vast information to Open Sharepoint site.
- Aviation Business Impact:
  - Data Leakage, Shadow-IT, Business Disruption (Ransomware or Malware can be distributed from the cloud), Regulatory Non-Compliance
- Likelihood Factors:
  - Lack of knowledge of cloud usage by employees or departments, lack of visibility and control of

Cloud Security Risks: Reducing the risk

- **People**: Provide users with all the tools they need from trusted sources. Education.
- **Technology**: Cloud Risk Assessments, Cloud Security Solutions, Data Loss Prevention
- **Process**: Govern and apply appropriate policies for managed or unmanaged device access to cloud Apps. Restrict access on a need to know basis. Detect and alert on anomalies of cloud App user logins, excessive downloads/uploads etc. Monitor privileged accounts and prevent unauthorized activity in IaaS instances

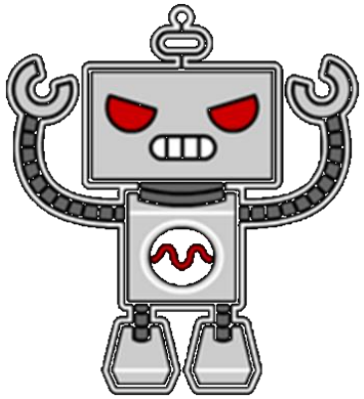
Return

SITA

BOT Attacks: Defining the Problem

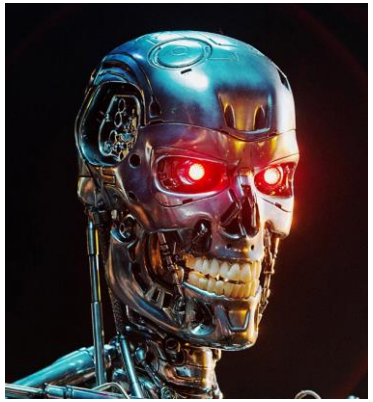
- Criminals and BOTs can use credentials (stolen or leaked), to access Airline Loyalty programs to sell FF miles and other perks. Competitors can also do “price scraping” wherein they do many price requests, driving up the “look-to-book” ratios and costing the carrier money.
  - Examples: Many, search Internet
- Aviation Business Impact
  - Loss of data, Loss of revenues, Additional costs, Reputational harm, Operational slowdown and increased costs (e-commerce sites serving BOTS)
- Likelihood factors
  - frequent flyer program (value of points: How many partners, how many places they fly), “hardness" of FF Program-number of methods of payment

Bad BOT Airline Targets



1. Criminals: Use stolen credentials for fraudulently buy tickets and access frequent flyer accounts

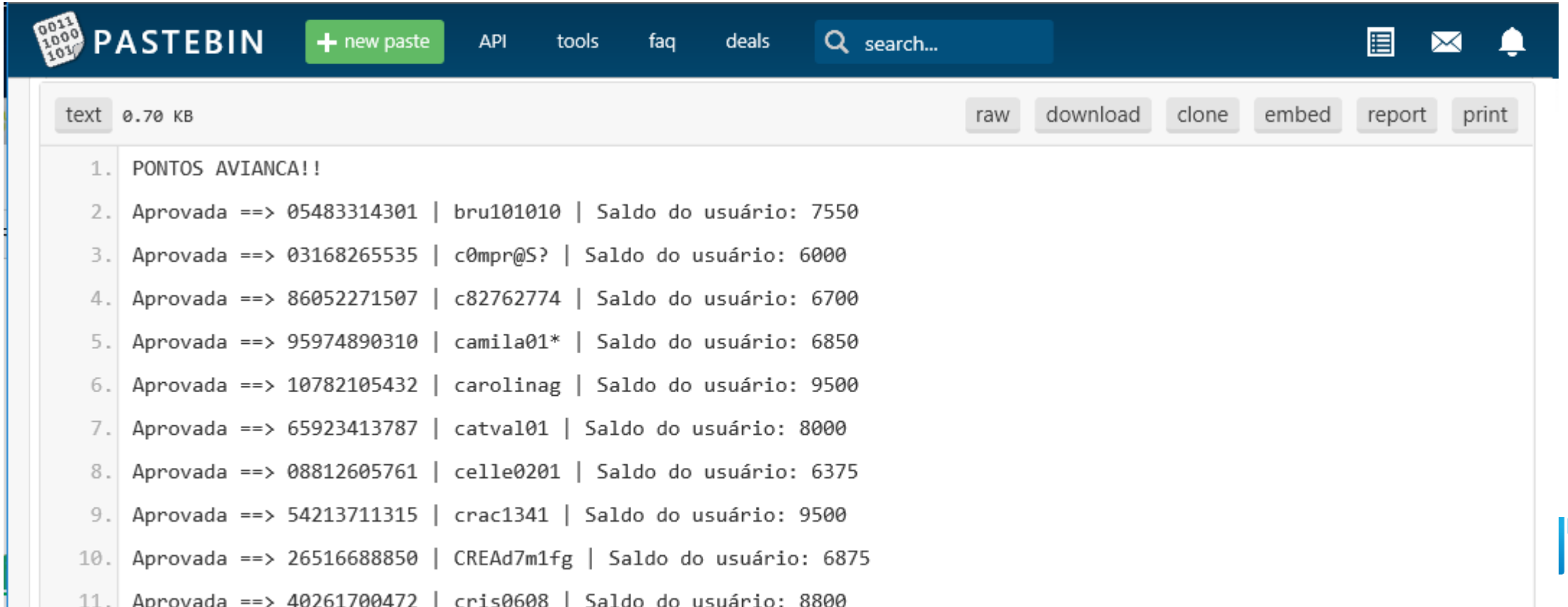
2. Online Travel Agents and Competitors: “Scrape” Content and Pricing from Airline Websites



DEMO! How BAT BOTs work

Spotify: https://pastebin.com/tji6B3eV

Spotify: https://pastebin.com/YBEawMMJ



Criminals: How BOTS attack FF programs

Step 1: Unrelated compromise of login credentials:

→ 2.3 Billion Credentials spilled in 2017

→ 15 Months between Spill and announcement

Source: Shape Security 2018 Credential Spill Report

Step 2: Program BOT to perform “Credential Stuffing” in Target Airlines FF Programs

Step 3: Upon Success, convert miles to flights, goods/services, debit cards

BOT Attacks: Reducing the risk

- **People**: User Training, avoid reusing passwords and make complex passwords. Avoid sharing too much on social media.
- **Technology**: Two-factor authentication (2FA), Use a fraud detection platform / BOT Mitigation Solution
- **Process**: “Normal" PCI compliance, Have an incident management process,

Return

IoT / IT/OT convergence defining the problem

- Description:
  - IoT greatly increases the attack surface. IoT devices are very basic and often cannot support clients for verification/authentication.
  - Operational Technology (OT), is continuously being automated and integrated within the IT environment. This makes for an attractive target for disruption-motivated hackers and makes OT accessible from the IT infrastructure.
- Examples: European Airport Baggage System hijacked by hackers, Asian A/P FIDs screen overwritten with insults to local politicians,
- Aviation Business Impact: Operational disruption
- Likelihood factors: Attack surface, cyber controls

IoT / IT/OT convergence Reducing the risk

- **People**: Automate/verify IT configurations
- **Technology**: Network Access Control
- **Process**: Network segmentation, asset discovery/classification/management-authentication- up to date device security patching. Automated security responses

Return

DDoS Defining the Problem

- A denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. A distributed denial-of-service (DDoS) is where the attack source is more than one, often thousands of, unique IP addresses.
- Examples:
  - Many, search Internet
- Aviation Business Impact
  - Flight departure delays, Disruption of operations, Revenue, Lost Sales, Reputation
- Likelihood factors
  - Public visibility, Public facing IPs, Limited bandwidth capacity

DDoS Reducing the risk

- **People**: N/A
- **Technology**: DDoS protection solution
- **Process**: Separate networks/subnets. Public/Private Internet Access, Perimeter Security Configurations

Return

Insider threat Defining the Problem

- Insider threat can be intentional or accidental. People are often the weakest link, or the biggest threat. Weakest link because they may not be aware of the risks, may click on links they should not or open attachments they shouldn't. They may make mistakes in configuring Firewalls, or leaving their PCs unlocked. Also, employees may have access to key information and systems and, given the right motivation, may use that access to ill-effect.
- Examples
  - Edward Snowden, See Examples of Phishing, and Ransomware, which can start with an unwitting employee. PenAir is an example of purposeful cyber attack by employee. Mistakes by IT and Cyber employees can be responsible for many breaches/attacks but often are not divulged as such.
- Aviation Business Impact:
  - Loss of data, operational disruption, reputational, revenue loss, IP Loss, PAX safety, "spying." According to Ponemon Institute 2018 Global Study on Cost of Insider Threats, total average cost per incident is $8.76 million, and it takes 2 months to resolve.
- Likelihood factors:
  - employee awareness, hostility / disgruntled / satisfaction, behavior monitoring/analysis, lack of DLP / Access Control, "political" nature of entity, global exposure

Insider threat: Reducing the risk

- **People**:
  - For general employees, see Phishing and Ransomware advice. End Users training, User behavior analytics
  - For IT Staff, Related Policies and Process
- **Technology**: Data Loss Prevention, Cloud Access Security Broker (CASB), Security Information and Event Management (SIEM), Account management.
- **Process**: Limit information on a need-to-know basis. Do not share passwords/logins. Exiting employees should have credentials immediately revoked.

Return

Supply Chain / 3rd Party

- Description: Risks that 3rd parties that provide services will not secure the data or systems access that they must be given.
- Examples: Australian Airport ID card Provider, Target (HVAC), Many, search Internet
- Aviation Business Impact: Many
- Likelihood factors: Number of third parties, what they have access to, partner security controls.

Questions you should ask your partners

- Do you have a security strategy?
- What is your Level of preparation with regards to new regulation (Data protection, regulations, critical infra…)?
- Have you identified all threat vectors and potential risks?
- Do you have an incident response plan? Is it tested?
- If so, has it proven effective when facing cyber attacks?
- …..

Return

What SITA Does

SITA Cyber Security

Aviation Cyber Security Challenges

Lack of understanding of business impact	**Limited knowledge of ATI among cyber providers**	**Large cyber risk and low budget**

SITA Proposition

Cyber Security Expertise

+

Deep Aviation Knowledge

=

A set of solutions specifically designed to address the needs of the air transport industry

SITA PORTFOLIO

CYBER SECURITY

Consulting Services

360° Airline Cyber Risk assessment
Maturity assessment
Incident response

Managed Services

SECURITY OPERATIONS CENTER
Aviation SOC & SOC advisory

MANAGED SECURITY APPLIANCES
Infra and Cloud Security

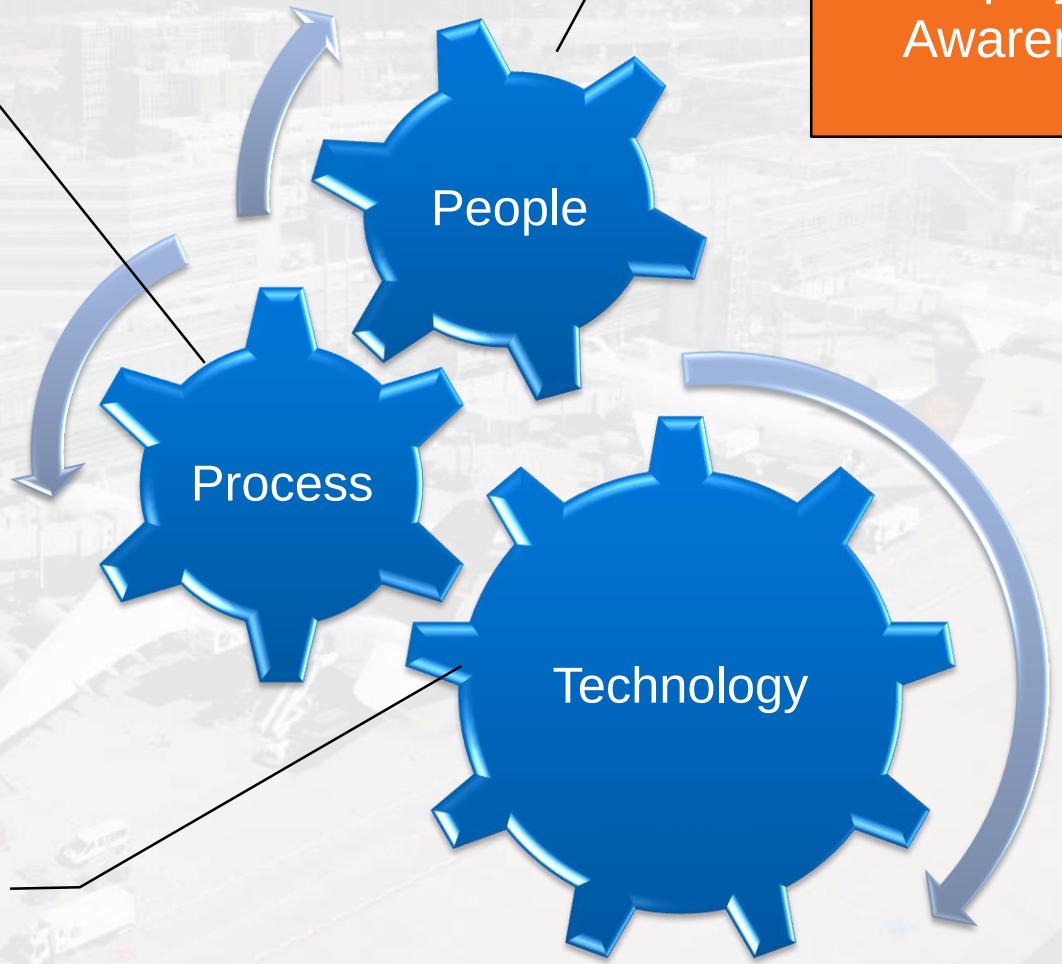
SITA

SITA UNIQUE AIRPORT TOOLS AND METHODOLOGY

We concentrated **70 years** of business expertise into one single Aviation specific cyber security **toolkit**.

- ISO-27001
- Network Design
- SW Development
- 2FA for Outlook
- Periodic testing/reviews
- Incident Response

- CISO Office
- Executive Management
- Employee Training and Awareness



- Physical Security
- Perimeter Security
- Defense in Depth
- PC Security
- Web Security
- Security Operations Center (SOC)
- ATI Threat Feed

Creating Community Value

Industry Collaboration

Foster increased **collaboration** for:

- collective defense to facilitate industry responses and mitigation of risks disruption to business

Cyber Threat Intel.

Support sharing of **actionable security info.** on emerging threats, vulnerabilities and techniques to:

- support their security management and risk mitigation activities

SITA

SITA Community Cyber Threat Center (CCTC)

- Cyber Threat Intelligence tailored for the ATI
- SITA Manages the platform
- Members may share information either anonymously or attributed to the organization
- Consolidates ATI-focused information and includes:
  1. Threat Intelligence Information and Advisories
  2. Customized Intelligence Alerts
  3. SITA weekly news and Cyber Threat Digest
  4. Invitations to calls/meetings/conferences on the subject

AVIATION CYBER SECURITY RECOMMENDED FRAMEWORK

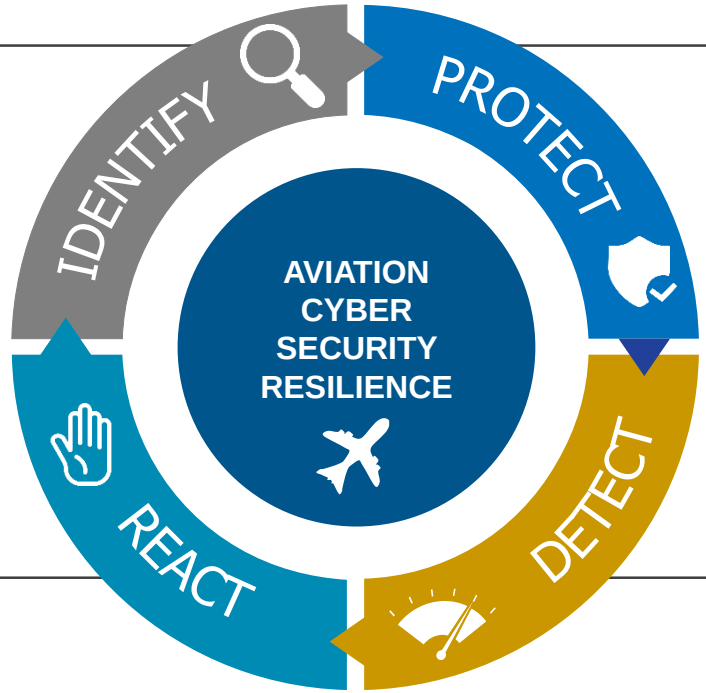
Aviation Framework

Identify aviation cyber risks

Develop the institutional understanding to manage cybersecurity risk to systems, assets, data, and capabilities

Protect Aviation critical assets

Risk mitigation controls and safeguard tailored to the Air Transport context and constraints.



React for business safeguard

Mitigate potential business impacts of an incident or eventually a crisis.

Detect Industry specific attacks

Tailored detection solutions and scenario to the aviation sector.

SITA

Aviation cyber security : good practices observed

1. Raise awareness with company board
2. Risk-based, top-down approach
3. Perform **cyber maturity assessments**
4. Prepare for real attacks to lower impact and cost
5. Update Processes, Tools, train people, measure
6. Perform distributed cyber risk assessments of suppliers
7. Adopt **industry cybersecurity** and data protection standards
8. Engage with peers, share and receive cyber intelligence

Final Word

Address CYBER risks as a community…

- Share threat intelligence
- Collaborate on initiatives
- Raise public awareness
- Partner with public sector and authorities