الإتحاد العربي للنقل الجوي
arab air carriers' organization

CYBER SECURITY

Securing Operations in a Multi-Stakeholder Environment

01 October 2019 - Kuwait

DEFINITION & STAKEHOLDERS

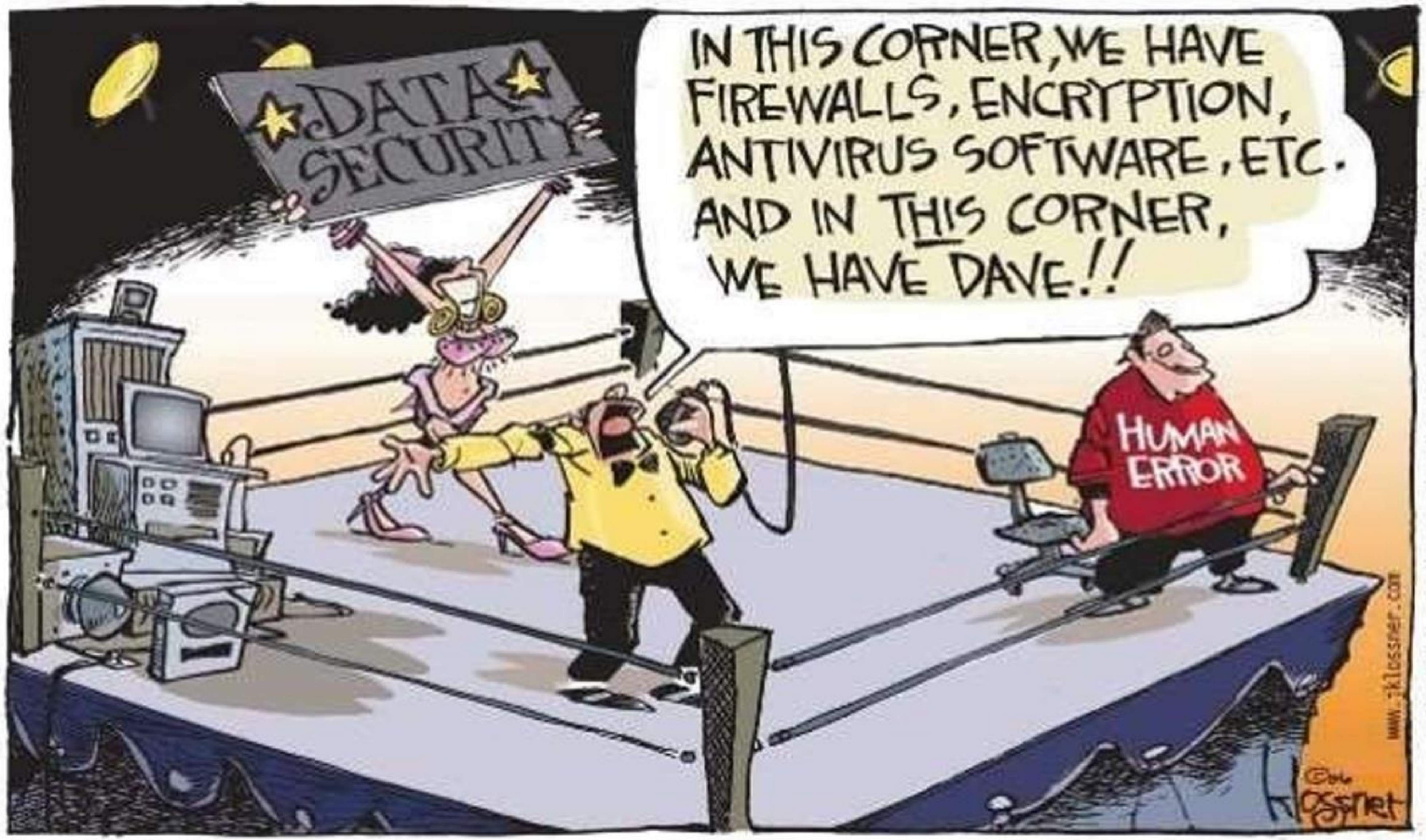
Cyber security comprises of controls (covering people, process and technology) designed to protect systems, networks and data from digital attacks.

Cyber Security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment as well as organizations' and users' assets. It encompasses the protection of electronic systems from malicious attacks and the means by which the consequences of such attacks should be handled.

Stakeholders involved include:

- ✓ Air Traffic Control Systems
- ✓ Airport Operators
- ✓ Airport Information Systems
- ✓ Aircraft operators
- ✓ Aircraft Systems
- ✓ Airport Tenants (Cargo, Duty Free, Catering, Ground Handling, etc…)
- ✓ Aircraft Manufacturers
- ✓ System Developers
- ✓ PEOPLE INVOLVED IN ALL THE ABOVE

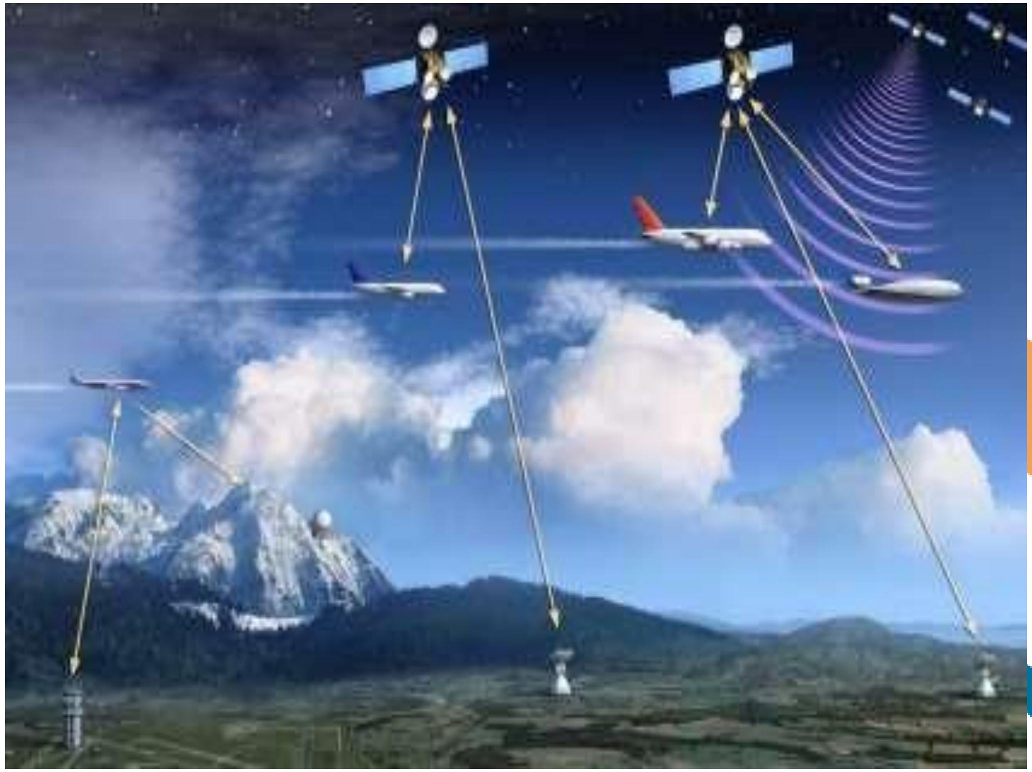
PEOPLE


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©06 Klossner

copyright 2006 john klossner, www.jklossner.com

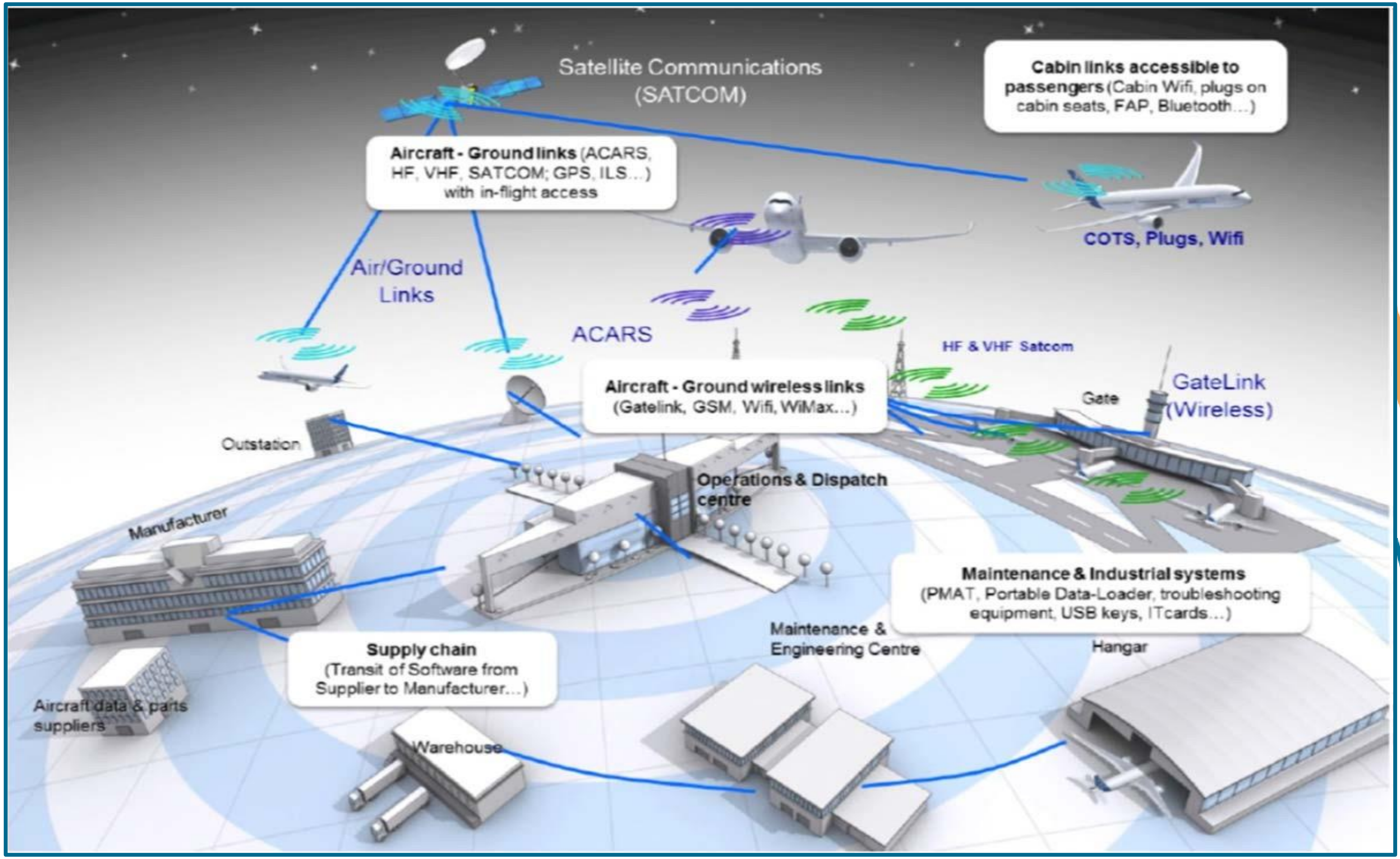
WHY CYBERSECURITY IN TECHNICAL DOMAINS

Over There!
Skilled Workers
On the ground behind the lines
In the Air Service
CHAUFFEURS WOOD WORKERS CARPENTERS
METAL WORKERS MACHINISTS TAILORS
AUTO MECHANICS PHOTOGRAPHERS MOTORCYCLISTS
AND MEN FROM 40 OTHER TRADES
Skilled Workers Registered in the Draft, or Under 40 Years of Age Can Still Join the
Aviation Section, Signal Corps, U.S. Army

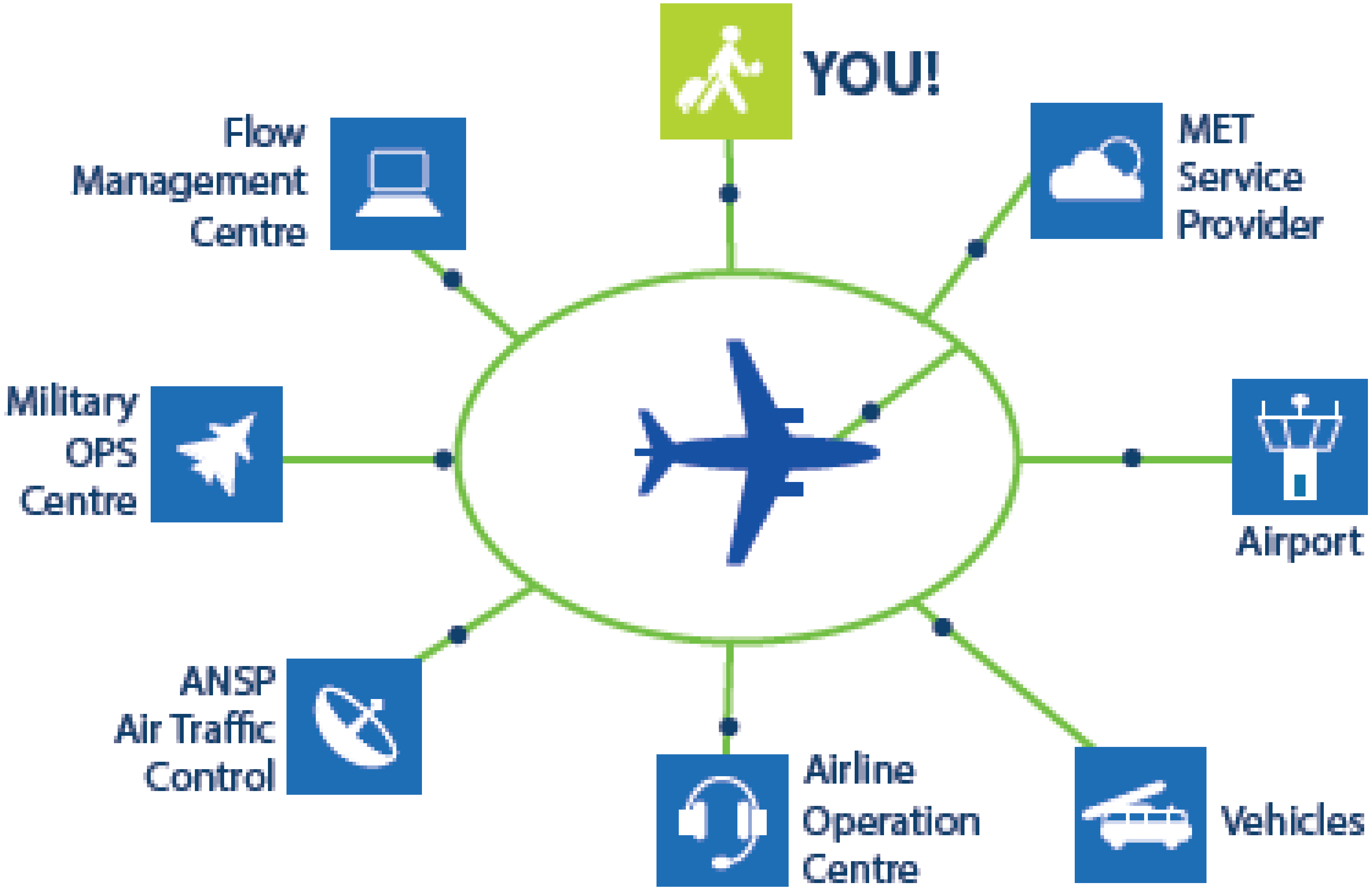


FROM THIS → TO THIS

CURRENT INFRASTRUCTURE


Satellite Communications
(SATCOM)
Cabin links accessible to passengers (Cabin Wifi, plugs on cabin seats, FAP, Bluetooth…)
Aircraft - Ground links (ACARS, HF, VHF, SATCOM; GPS, ILS…) with in-flight access
COTS, Plugs, Wifi
Air/Ground Links
ACARS
HF & VHF Satcom
Aircraft - Ground wireless links (Gatelink, GSM, Wifi, WiMax…)
Gate
GateLink (Wireless)
Outstation
Operations & Dispatch centre
Manufacturer
Maintenance & Industrial systems (PMAT, Portable Data-Loader, troubleshooting equipment, USB keys, ITcards…)
Maintenance & Engineering Centre
Hangar
Supply chain (Transit of Software from Supplier to Manufacturer…)
Aircraft data & parts suppliers
Warehouse

FUTURE INFRASTRUCTURE



YOU!

Flow Management Centre

MET Service Provider

Military OPS Centre

Airport

ANSP Air Traffic Control

Airline Operation Centre

Vehicles

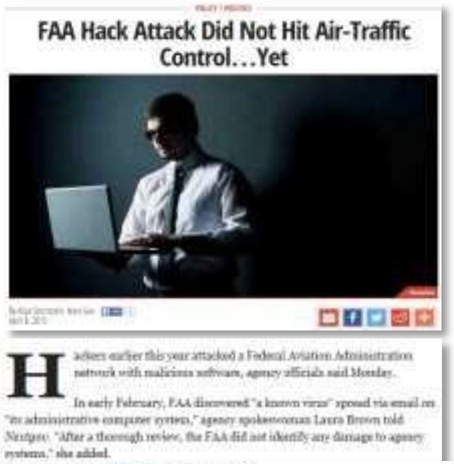
IN TERMS OF SECURITY TERMINOLOGY

Threat

=

CAPABILITY ✖ INTENT

SOME EXAMPLES



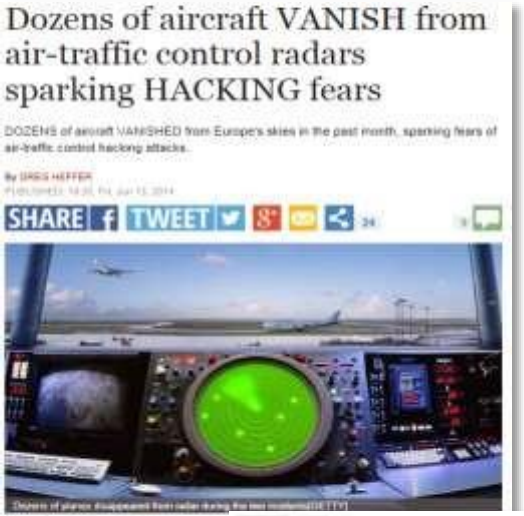
FAA Hack Attack Did Not Hit Air-Traffic Control…Yet

Hackers earlier this year attacked a Federal Aviation Administration network with malicious software, agency officials said Monday.

In early February, FAA discovered "a known virus" spread via email on "its administrative computer system," agency spokeswoman Laura Brown told Nextgov. "After a thorough review, the FAA did not identify any damage to agency systems," she added.

An upcoming com
center might be a
award notice that

Related: Congr



Dozens of aircraft VANISH from air-traffic control radars sparking HACKING fears

DOZENS of aircraft VANISHED from Europe's skies in the past month, sparking fears of air-traffic control hacking attacks.

By GREG HEFFER
PUBLISHED: 14:35, Fri, Jun 13, 2014

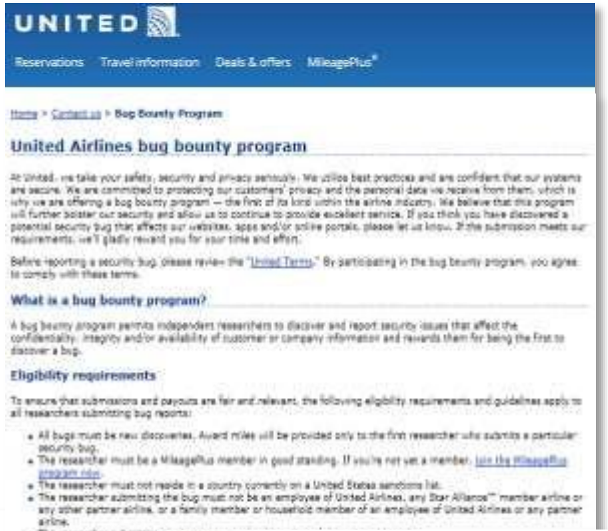
SHARE f TWEET 34

Dozens of planes disappeared from radar during the two incidents[GETTY]

Air-traffic controllers in Austria, Germany, t
planes' position, direction, height or speed

Despite the cases of vanishing aircraft on t
serious danger to passengers on the aircra

There have been suggestions the disappea
attack.



UNITED

Reservations Travel information Deals & offers MileagePlus®

Home > Contact us > Bug Bounty Program

United Airlines bug bounty program

At United, we take your safety, security and privacy seriously. We utilize best practices and are confident that our systems are secure. We are committed to protecting our customers' privacy and the personal data we receive from them, which is why we are offering a bug bounty program — the first of its kind within the airline industry. We believe that this program will further bolster our security and allow us to continue to provide excellent service. If you think you have discovered a potential security bug that affects our websites, apps and/or online portals, please let us know. If the submission meets our requirements, we'll gladly reward you for your time and effort.

Before reporting a security bug, please review the "United Terms." By participating in the bug bounty program, you agree to comply with these terms.

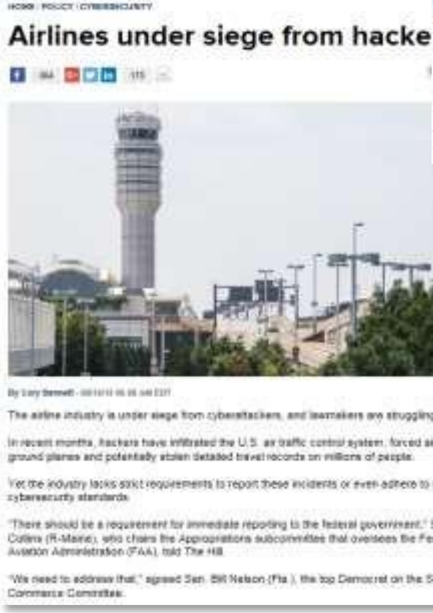
What is a bug bounty program?

A bug bounty program permits independent researchers to discover and report security issues that affect the confidentiality, integrity and/or availability of customer or company information and rewards them for being the first to discover a bug.

Eligibility requirements

To ensure that submissions and payouts are fair and relevant, the following eligibility requirements and guidelines apply to all researchers submitting bug reports:

- All bugs must be new discoveries. Award miles will be provided only to the first researcher who submits a particular security bug.
- The researcher must be a MileagePlus member in good standing. If you're not yet a member, join the MileagePlus program now.
- The researcher must not reside in a country currently on a United States sanctions list.
- The researcher submitting the bug must not be an employee of United Airlines, any Star Alliance™ member airline or any other partner airline, or a family member or household member of an employee of United Airlines or any partner airline.
- The researcher submitting



HOME | POLICY | CYBERSECURITY

Airlines under siege from hacke

By Cory Bennett - [illegible]

Getty Images

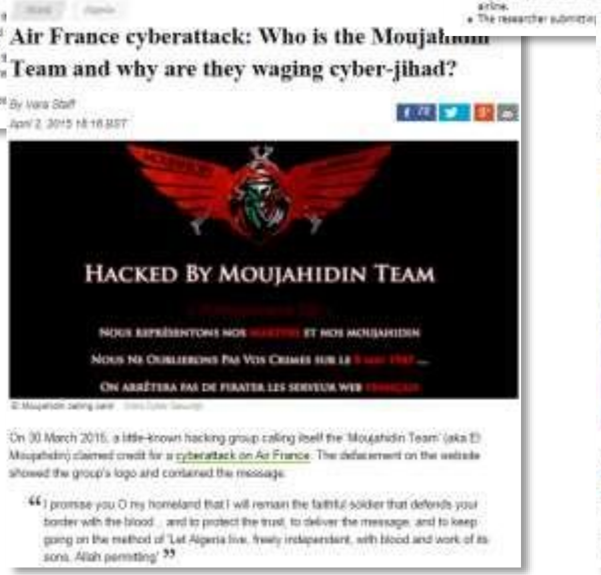
The airline industry is under siege from cyberattackers, and lawmakers are struggling to help.

In recent months, hackers have infiltrated the U.S. air traffic control system, forced airlines to ground planes and potentially stolen detailed travel records on millions of people.

Yet the industry lacks strict requirements to report these incidents or even adhere to specific cybersecurity standards.

"There should be a requirement for immediate reporting to the federal government," Sen. Susan Collins (R-Maine), who chairs the Appropriations subcommittee that oversees the Federal Aviation Administration (FAA), told The Hill.

"We need to address that," agreed Sen. Bill Nelson (Fla.), the top Democrat on the Senate Commerce Committee.



Air France cyberattack: Who is the Moujahidin Team and why are they waging cyber-jihad?

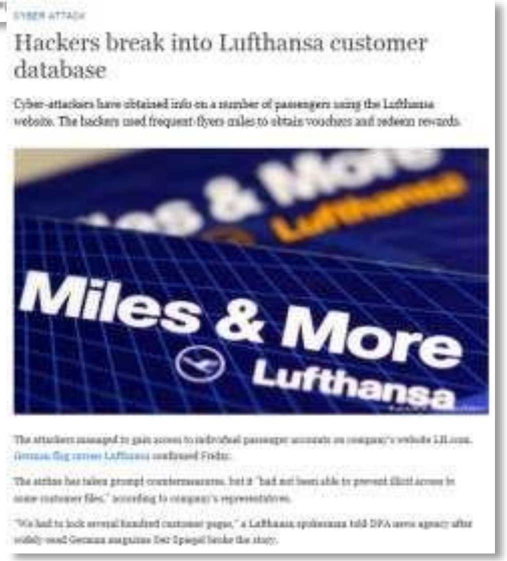
By Vara Staff
April 2, 2015 18:18 BST

HACKED BY MOUJAHIDIN TEAM
NOUS REPRÉSENTONS NOS [illegible] ET NOS MOUJAHIDIN
NOUS NE OUBLIERONS PAS VOS CRIMES SUR LE [illegible] …
ON ARRÊTERA PAS DE PIRATER LES SERVEUR WEB [illegible]

© Moujahidin calling card

On 30 March 2015, a little-known hacking group calling itself the 'Moujahidin Team' (aka El Moujahidin) claimed credit for a cyberattack on Air France. The defacement on the website showed the group's logo and contained the message:

> "I promise you O my homeland that I will remain the faithful soldier that defends your border with the blood … and to protect the trust, to deliver the message, and to keep going on the method of 'Let Algeria live, freely independent, with blood and work of its sons, Allah permitting' "



CYBER ATTACK

Hackers break into Lufthansa customer database

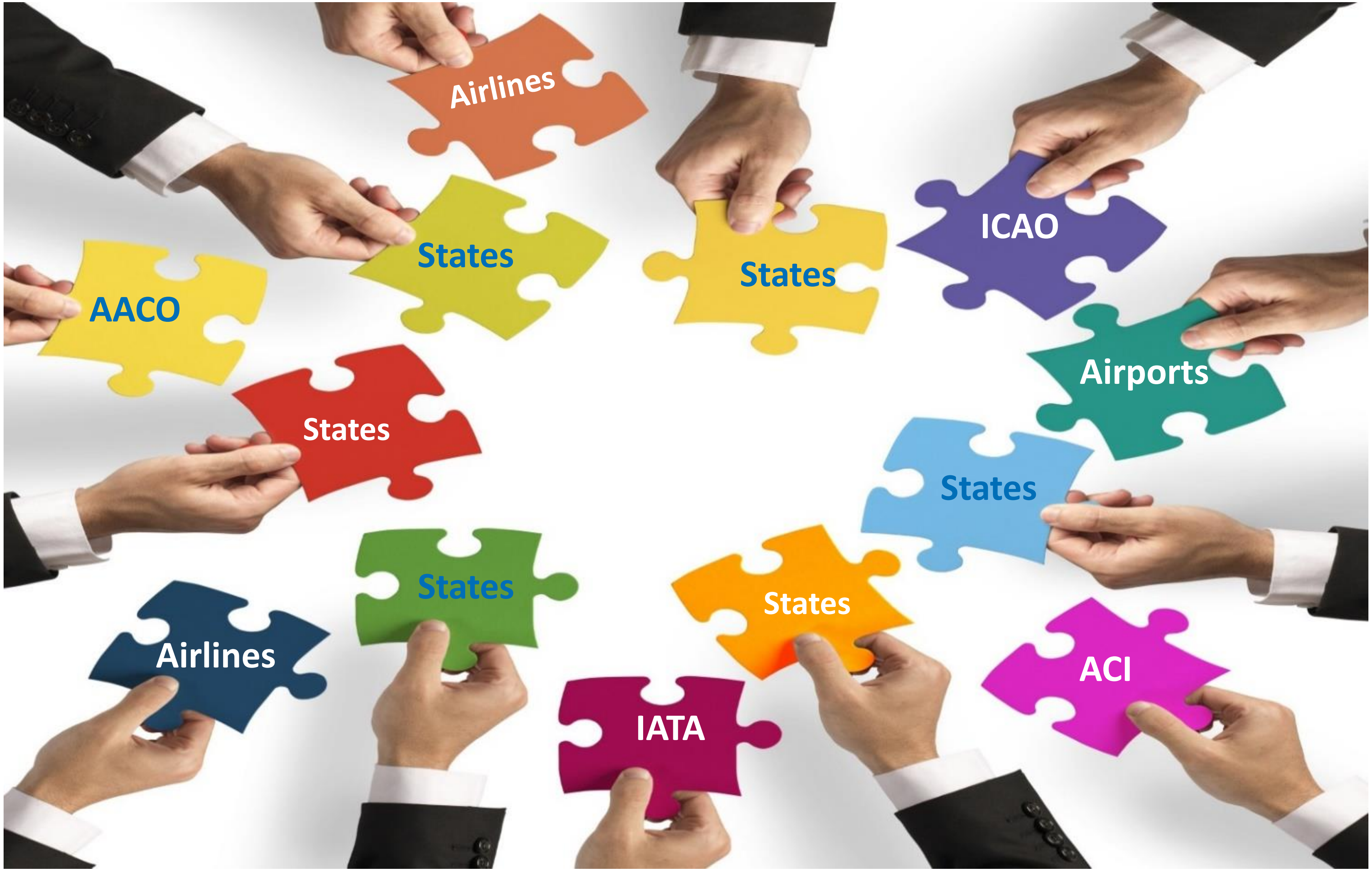
Cyber-attackers have obtained info on a number of passengers using the Lufthansa website. The hackers used frequent-flyers miles to obtain vouchers and redeem rewards.

The attackers managed to gain access to individual passenger accounts on company's website LH.com, German flag carrier Lufthansa confirmed Friday.

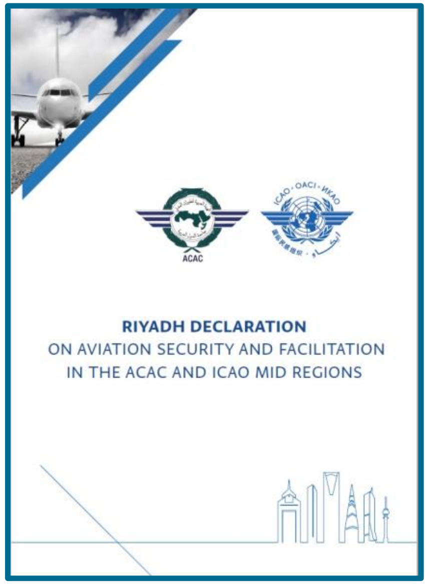
The airline has taken prompt countermeasures, but it "had not been able to prevent illicit access to some customer files," according to company's representatives.

"We had to lock several hundred customer pages," a Lufthansa spokesman told DPA news agency after widely-read German magazine Der Spiegel broke the story.

COLLABORATION IS KEY



GLOBAL/REGIONAL EFFORTS TO ADDRESS CYBER SECURITY



RIYADH DECLARATION
ON AVIATION SECURITY AND FACILITATION
IN THE ACAC AND ICAO MID REGIONS

DECLARATION ON CYBERSECURITY IN CIVIL AVIATION

DUBAI, UNITED ARAB EMIRATES

4 TO 6 APRIL 2017

We the Officials and representatives from the States and regnal and international organizations listed in the Annex, participating in the summit on cyber security in civil aviation convened by the International Civil Aviation Organization (ICAO) in Dubai, United Arab Emirates from 4 to 6 April 2017, to address challenges to aviation resulting from cyber threats;

Recalling the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation*, and the *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft* Done at Beijing on 10 September 2010 (Beijing Instruments);

Recalling further the ICAO Assembly Resolution A39-19: Addressing Cybersecurity in Civil Aviation, and the importance and urgency of protecting civil aviation's critical infrastructure systems and data against cyber threats by, inter alia:

a) implementing global, regional and State-level strategies on cybersecurity in civil aviation based on a shared vision;

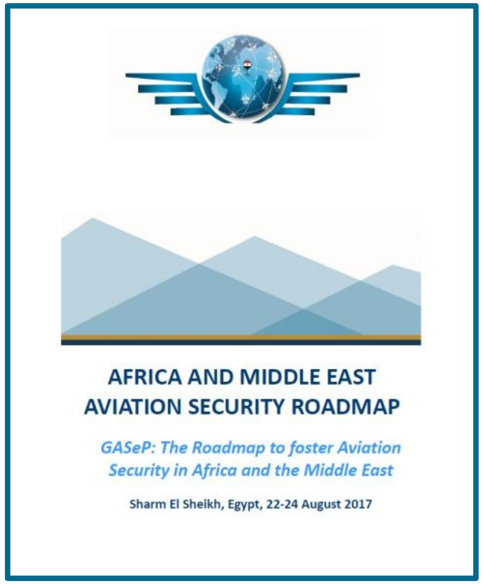
b) increasing the resilience of the global aviation system against cyber threats that may jeopardize the safety, security and efficiency of civil aviation; and

c) reaffirming the prominent role of ICAO as aviation's highest-level forum for addressing collaboratively cybersecurity in civil aviation;

Mindful of the challenges in safeguarding civil aviation against cyber threats in a demanding and continuously evolving aviation cybersecurity environment;

Noting that in many cyber incidents affecting the safety and security of civil aviation, their actors are focused on malicious intent, disruption of business continuity and theft of information for political, financial or other motivations;

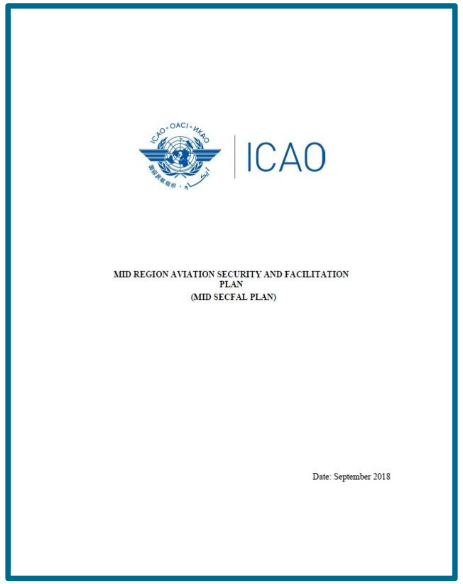
Recognizing that cyber incidents can affect critical civil aviation systems worldwide with catastrophic consequences, including the availability of information and communications technology systems, and the integrity and confidentiality of data, all of which the aviation sector is increasingly reliant on; and Considering the need to facilitate and encourage initiatives worldwide aimed at addressing cybersecurity in a collaborative, comprehensive and cross-cutting manner;



AFRICA AND MIDDLE EAST
AVIATION SECURITY ROADMAP

GASeP: The Roadmap to foster Aviation Security in Africa and the Middle East

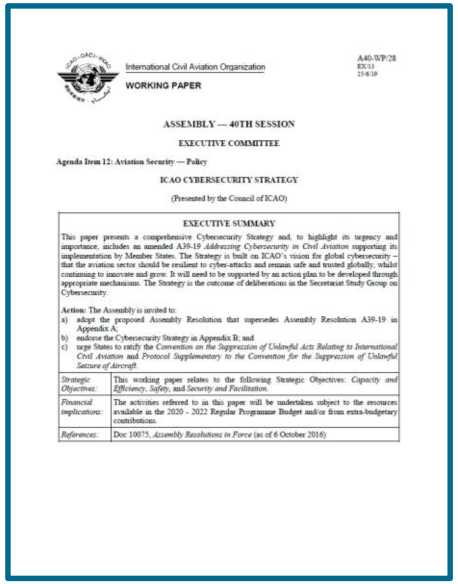
Sharm El Sheikh, Egypt, 22-24 August 2017



ICAO

MID REGION AVIATION SECURITY AND FACILITATION PLAN
(MID SECFAL PLAN)

Date: September 2018



International Civil Aviation Organization

WORKING PAPER

A40-WP/28
EX/13
25/6/19

ASSEMBLY — 40TH SESSION

EXECUTIVE COMMITTEE

Agenda Item 12: Aviation Security — Policy

ICAO CYBERSECURITY STRATEGY

(Presented by the Council of ICAO)

EXECUTIVE SUMMARY

This paper presents a comprehensive Cybersecurity Strategy and, to highlight its urgency and importance, includes an amended A39-19 *Addressing Cybersecurity in Civil Aviation* supporting its implementation by Member States. The Strategy is built on ICAO's vision for global cybersecurity – that the aviation sector should be resilient to cyber-attacks and remain safe and trusted globally, whilst continuing to innovate and grow. It will need to be supported by an action plan to be developed through appropriate mechanisms. The Strategy is the outcome of deliberations in the Secretariat Study Group on Cybersecurity.

Action: The Assembly is invited to:
a) adopt the proposed Assembly Resolution that supersedes Assembly Resolution A39-19 in Appendix A;
b) endorse the Cybersecurity Strategy in Appendix B; and
c) urge States to ratify the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* and *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft.*

Strategic Objectives:	This working paper relates to the following Strategic Objectives: *Capacity and Efficiency*, *Safety*, and *Security and Facilitation.*
Financial implications:	The activities referred to in this paper will be undertaken subject to the resources available in the 2020 - 2022 Regular Programme Budget and/or from extra-budgetary contributions.
References:	Doc 10075, *Assembly Resolutions in Force* (as of 6 October 2016)