ATM's database cybersecurity

Cybersecurity Awareness Presentation

- NAM/CAR AIDC
- AIDC/NAM/ICD/4

By CyberInflight

March 10, 2021 by Florent Rizzo

florent.rizzo@cyberinflight.com

www.cyberinflight.com

CyberInflight

01 Cyber-threat landscape

02 Market analysis

03 AIDC protocol and data security

04 Wrap ups & takeaways

About CyberInflight

Unique player in Aerospace Cybersecurity Market Intelligence

Independent company, employee owned

Founded in 2019 in France, headquartered in Toulouse

Specialized in the Aerospace market
(Airlines, airports, OEMs, ANSPs, industry players, cybersecurity solutions providers etc.)

Provides **Aerospace Cybersecurity Intelligence** through different forms

Strategic research reports

Training, cybersecurity awareness session

Ad-hoc consulting and advisory missions

Constant market monitoring

CyberInflight

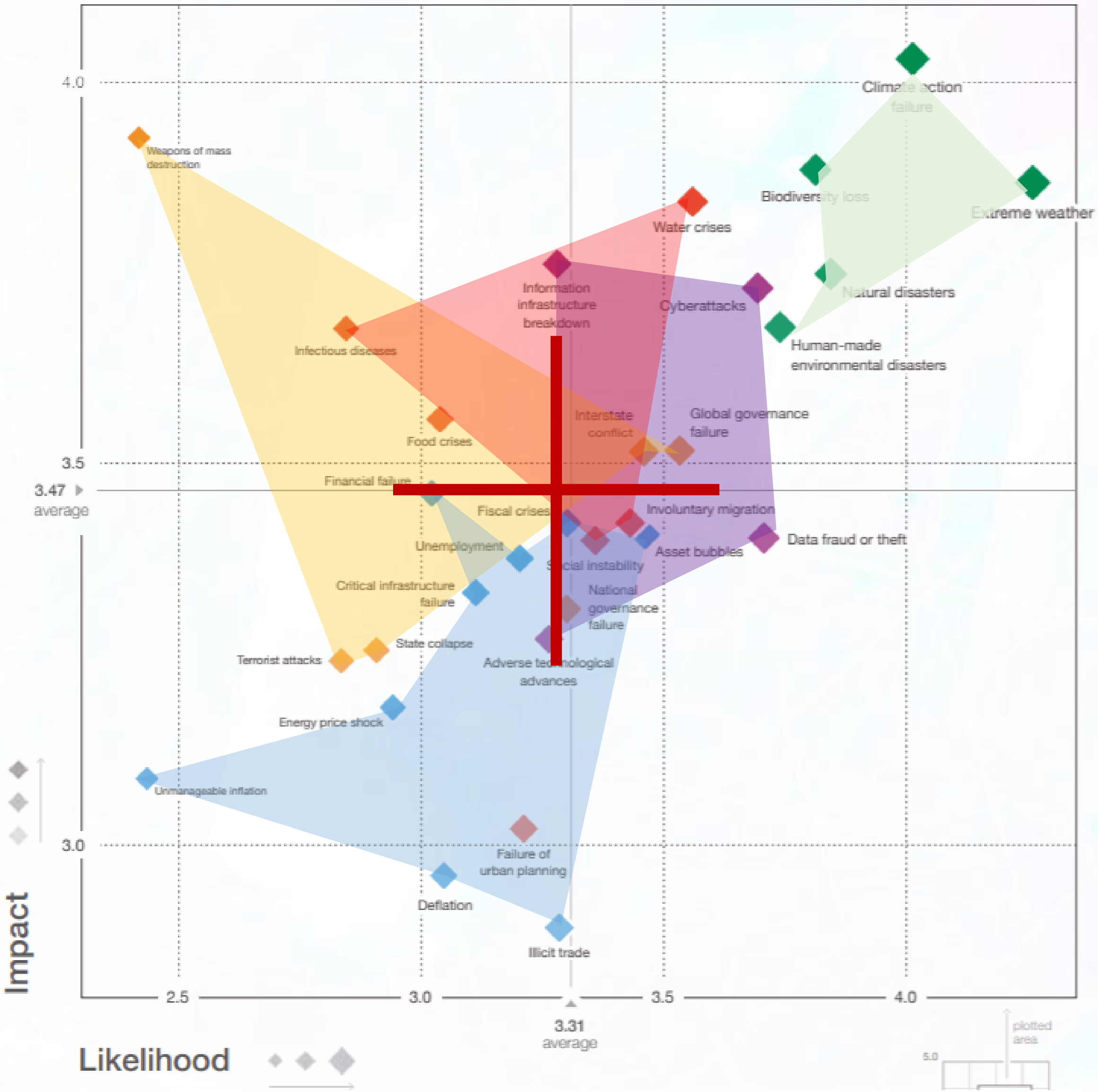
About me

- Founder of CyberInflight
- Consultant & Market Analyst
- Exp. French Civil Aviation (DGAC)
- Exp. Inflight connectivity
- Exp. Aerospace cybersecurity
- A350 avionic development background
- Involved in ANSPs protocol developments (RENAR-IP, FMTP, RWSL., space-based ADS-B…
- Aerospace enthusiast ☺

01

The cyberthreat landscape

Global risk landscape



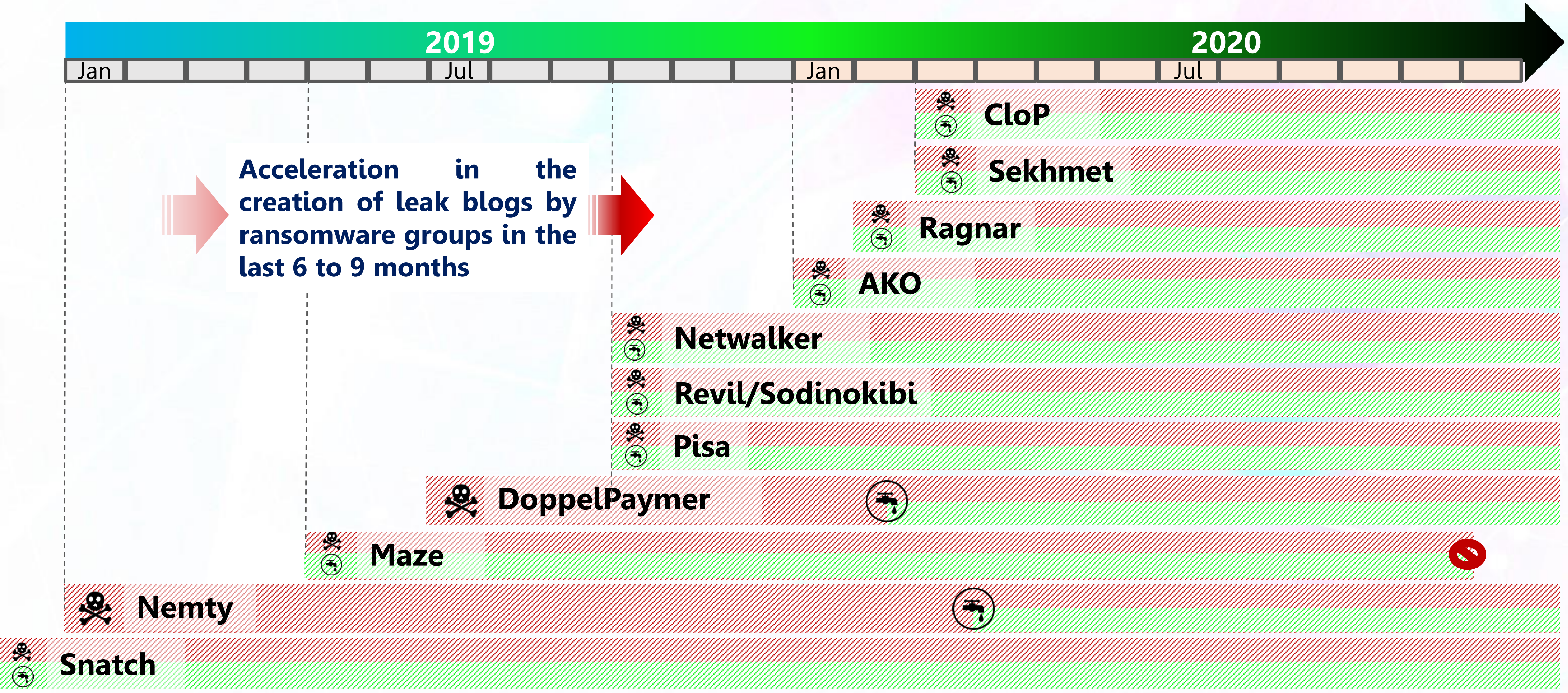
Global risk report 2020 from the World Economic Forum about the cyber-risks:

Among the **top-5 challenges for the world to face** in the next 10-years

Moving into the **high impact/high likelihood** quadrant

- ◆ Economic
- ◆ Environmental
- ◆ Geopolitical
- ◆ Societal
- ◆ Technological

Soar of darkweb blogs leaking corporate data



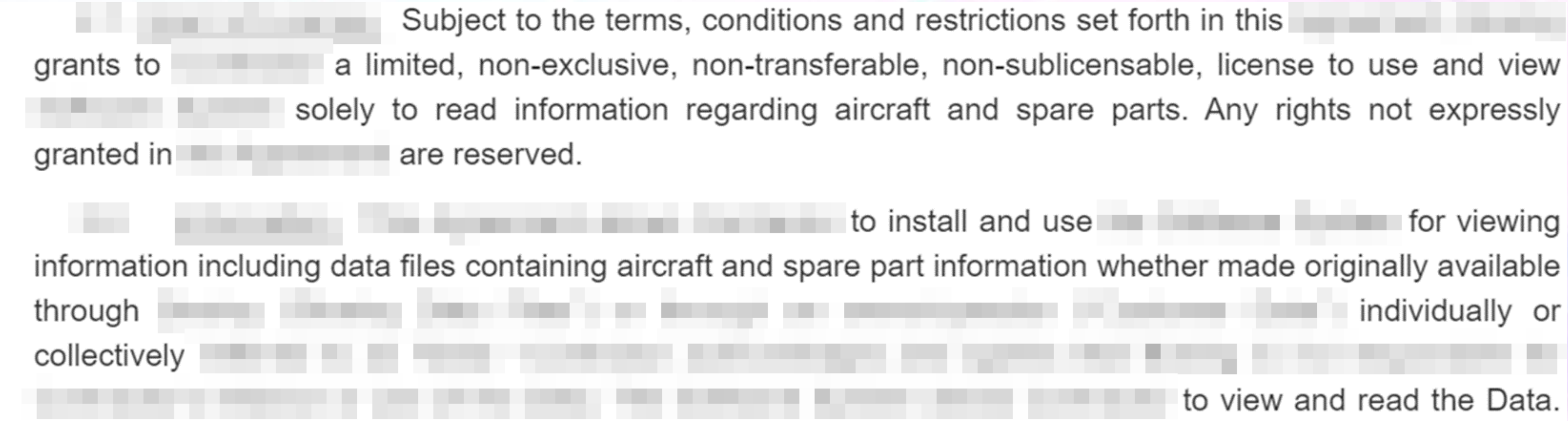
Acceleration in the creation of leak blogs by ransomware groups in the last 6 to 9 months

☠ Known date for starting operations by the ransomware group

Known date for the opening of data leak website or blog by the ransomware group

Example of unprotected aerospace databases (1/2)

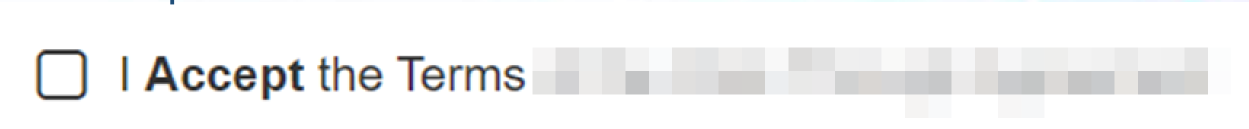
1. Web interface of a server from a stakeholder



[redacted] Subject to the terms, conditions and restrictions set forth in this [redacted] grants to [redacted] a limited, non-exclusive, non-transferable, non-sublicensable, license to use and view [redacted] solely to read information regarding aircraft and spare parts. Any rights not expressly granted in [redacted] are reserved.

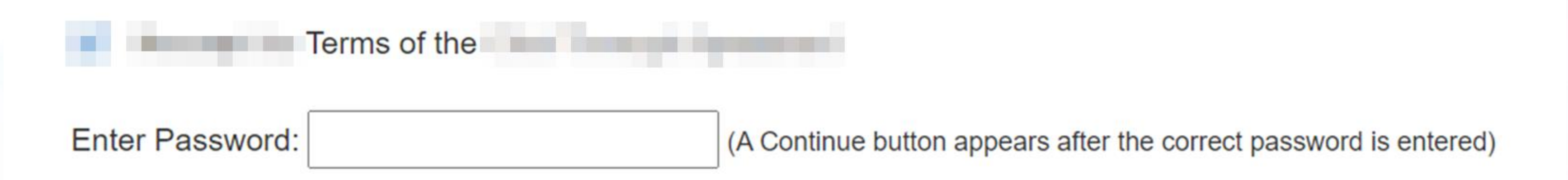
[redacted] to install and use [redacted] for viewing information including data files containing aircraft and spare part information whether made originally available through [redacted] individually or collectively [redacted] to view and read the Data.

2. The tick box allows to accept the Terms and Conditions



☐ I **Accept** the Terms [redacted]

3. Ticking the box asks for a password. The website was recently secured in xxx 2020, for obvious reasons, as it was left open, without password before that date.

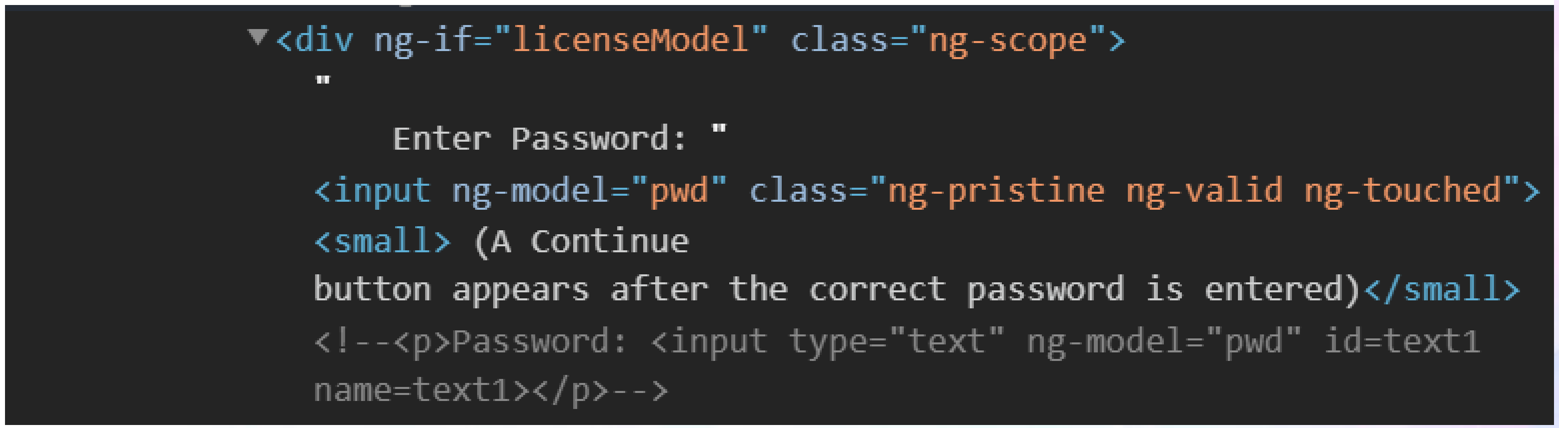


[redacted] Terms of the [redacted]

Enter Password: ____________ (A Continue button appears after the correct password is entered)

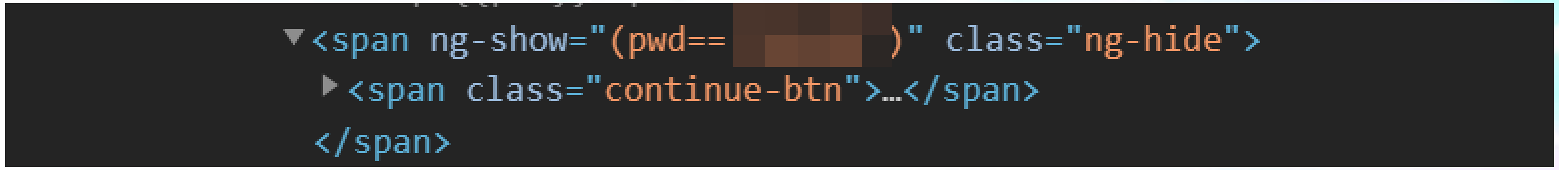
Example of unprotected aerospace databases (2/2)

4. Display the code of the web page



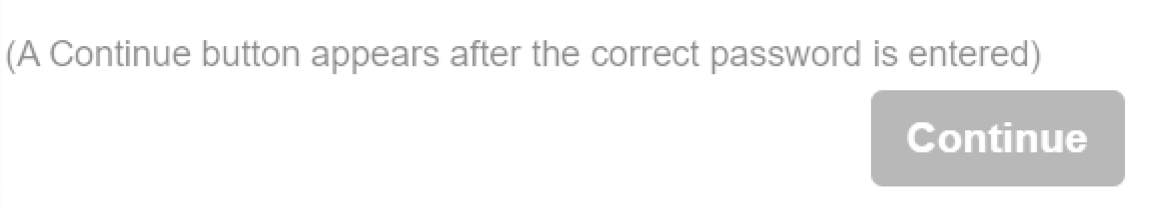
```
▼<div ng-if="licenseModel" class="ng-scope">
   "
       Enter Password: "
   <input ng-model="pwd" class="ng-pristine ng-valid ng-touched">
   <small> (A Continue
   button appears after the correct password is entered)</small>
   <!--<p>Password: <input type="text" ng-model="pwd" id=text1
   name=text1></p>-->
```

5. Read the password in clear text !



```
▼<span ng-show="(pwd==[redacted])" class="ng-hide">
  ▶<span class="continue-btn">…</span>
 </span>
```

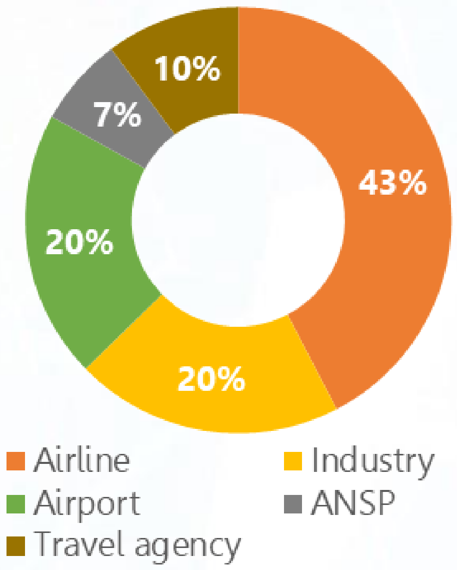
6. Use the password and the “continue” button appears



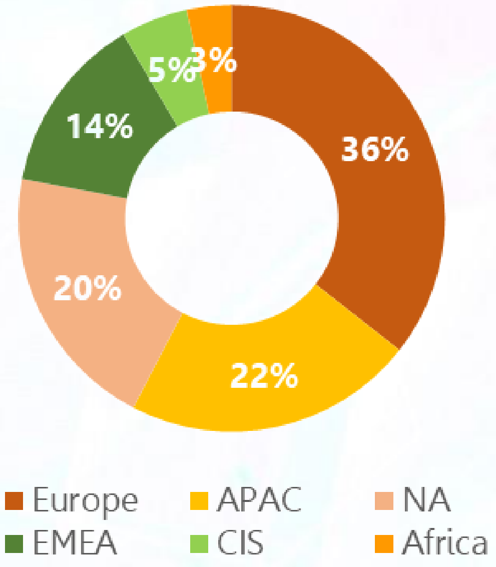
(A Continue button appears after the correct password is entered)

Cyberthreat on aerospace in 2019

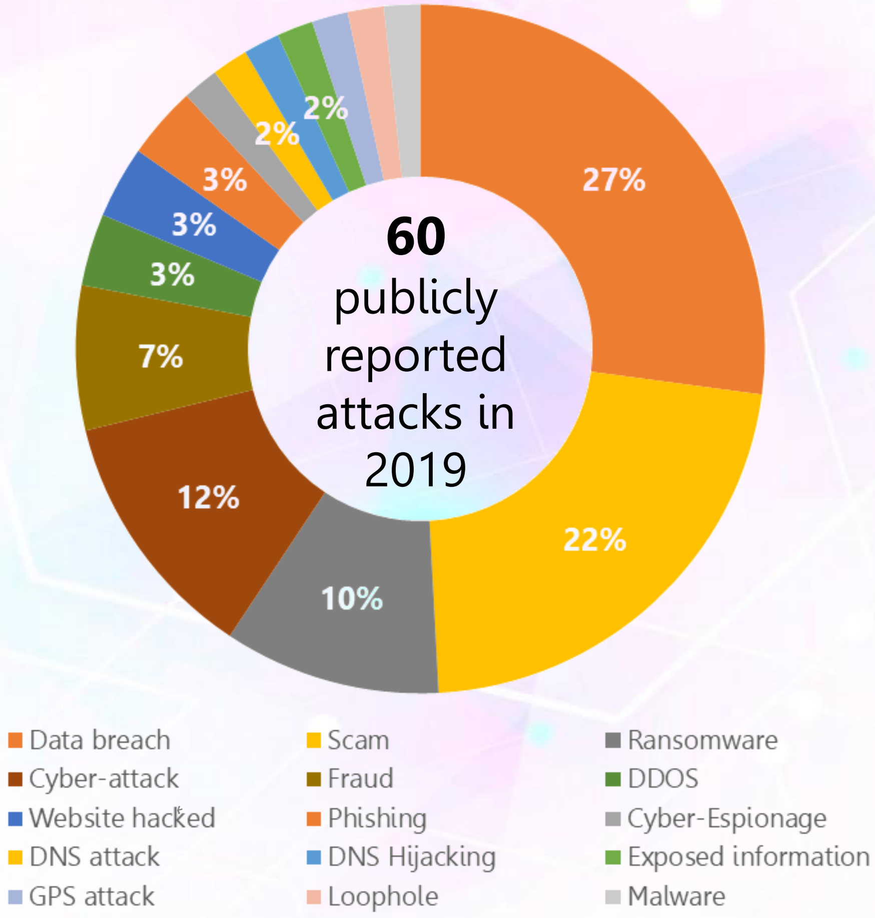
CYBERATTACKS BY TARGET TYPE



CYBERATTACKS BY REGION

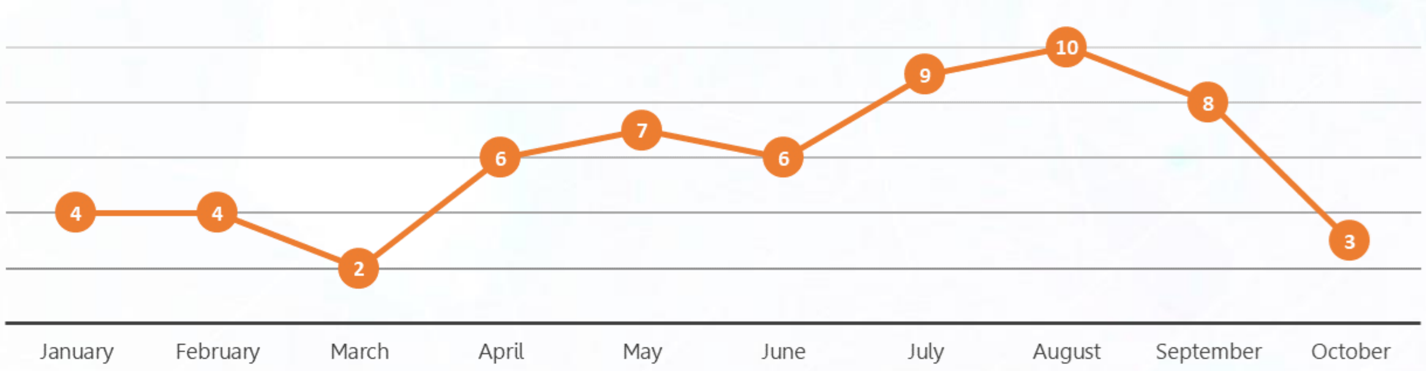


CYBERATTACKS BY TYPE OF ATTACK



**Cyber-attack: no information is given to categorize the attack. It can results in data breach or disruption.*

NUMBER OF CYBERATTACKS BY MONTH



Source EATM-CERT: based on 60 cases of cyber attacks perpetuated in 2019 (no data for November and December)

Cyberthreat on aerospace in 2020

Cyberattack hits Alaskan airline **RavnAir,** Dec. 2019

New York Airport hit by cyber attack during Christmas, Dec. 2019

Transavia data leak, Feb. 2020

Brussel Airline booking app. Hijacking, Mar. 2020

Cyberattack against **Sarrebruck airport** and the state holding company, Saar GmbH, Mar 2020

ST Engineering major ransomware attack, reported June 2020

Impersonation of aerospace companies on LinkedIn by a hacker group, June 2020

San Francisco Airport data breach, Apr. 2020

Air transport and governments hits by cyberattacks, May 2020

PAX information sold by Israeli flight attendant Reported: June 2020

Ransomware attack on **NASA** subcontractor, June 2020

Iranian hackers aiming to steal aerospace satellite data Sept. 2020

Hackers attack Airport AWOS system. Sept 2020

Cyberattack on **FlightRadar24**, Sept. 2020

Cyber attack grounds **Transport Malta** systems, Oct. 2020

German IT company hit by ransomware. Sept. 2020

United Airlines website flaw, Sept 2020

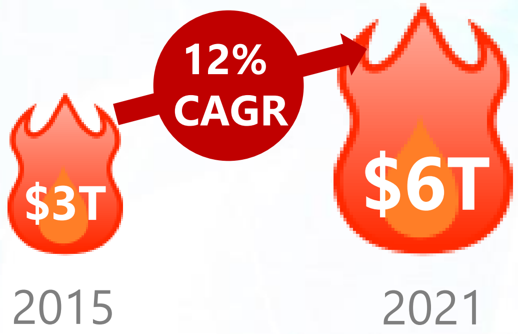
Airlink international UAE leaked data. Oct 2020

And others with indirectly related to aerospace…

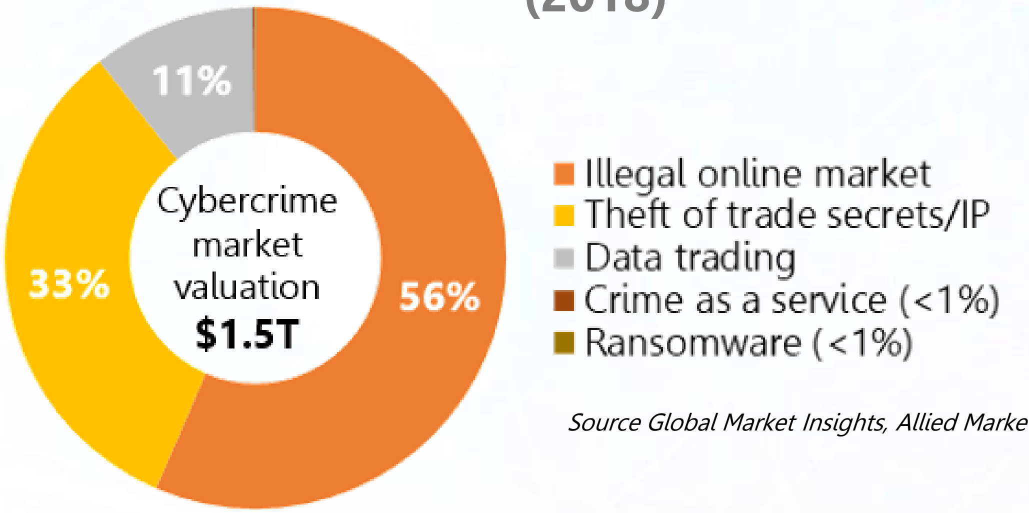
On the BLACK HAT side *(public info.)*

Cybercrime economy

CYBERCRIME DAMAGES TO THE WORLD

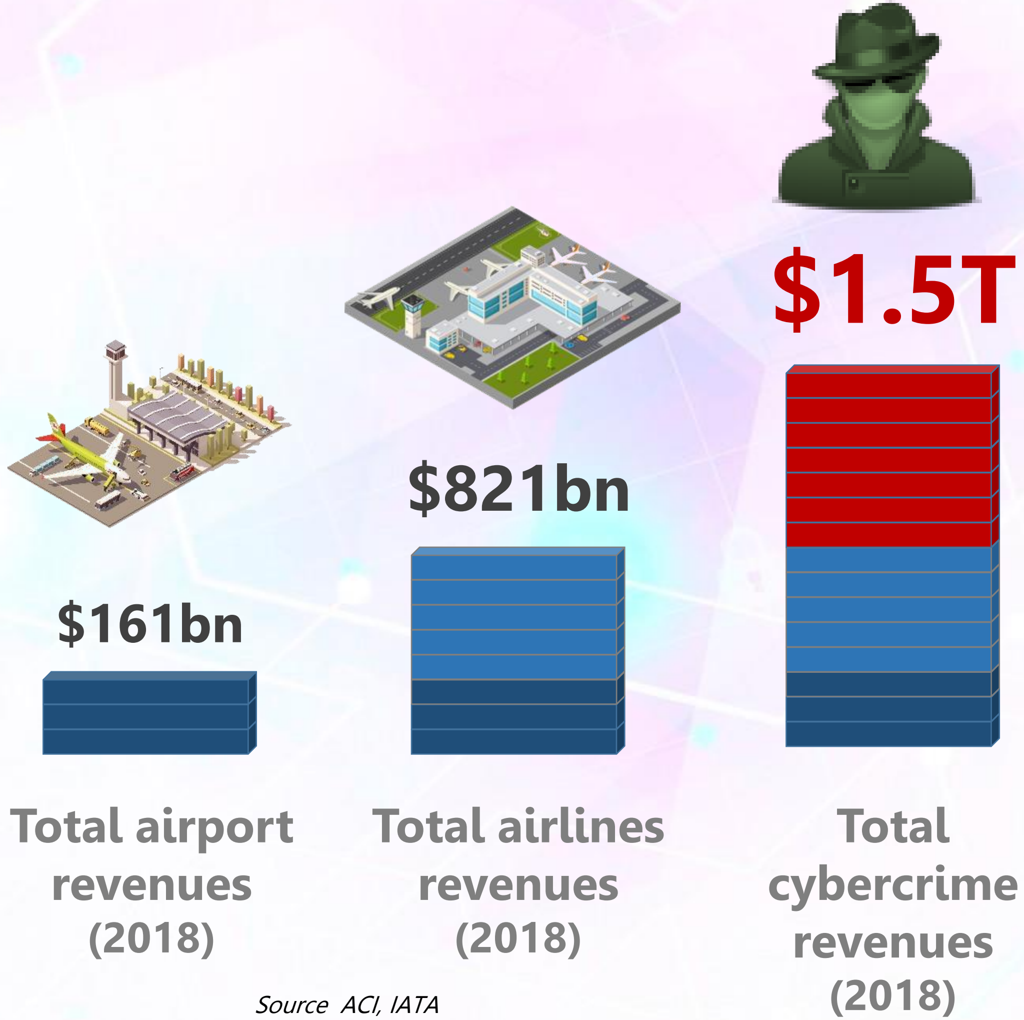


ILLICIT PROFIT (2018)



Source Global Market Insights, Allied Market Research, Bromium

INDUSTRIES REVENUES IN PERPECTIVE



Source ACI, IATA

Cybersecurity principles to apply

100% SECURITY IS IMPOSSIBLE

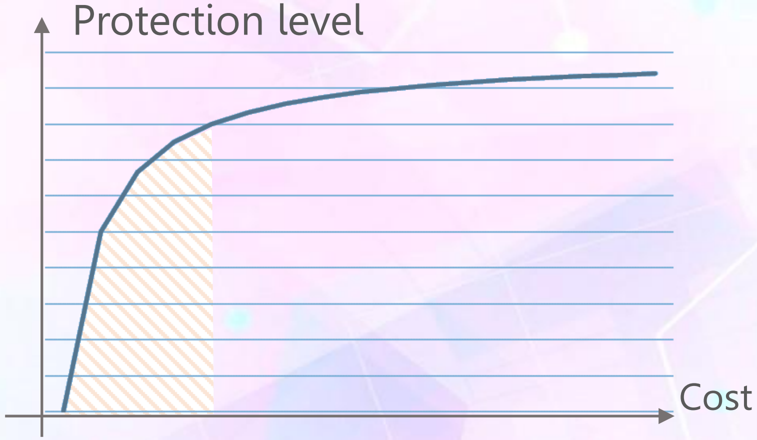
99.99%

Security comes with a cost

AN UNFAIR GAME

Attacker has to win once
Defenders always have to win

PARETO'S LAW APPLIES



20% of cybersecurity measures
may cover 80% of cyberattacks

KERCKHOFF'S PRINCIPLE

"The enemy knows the system"

A LAYERED APPROACH

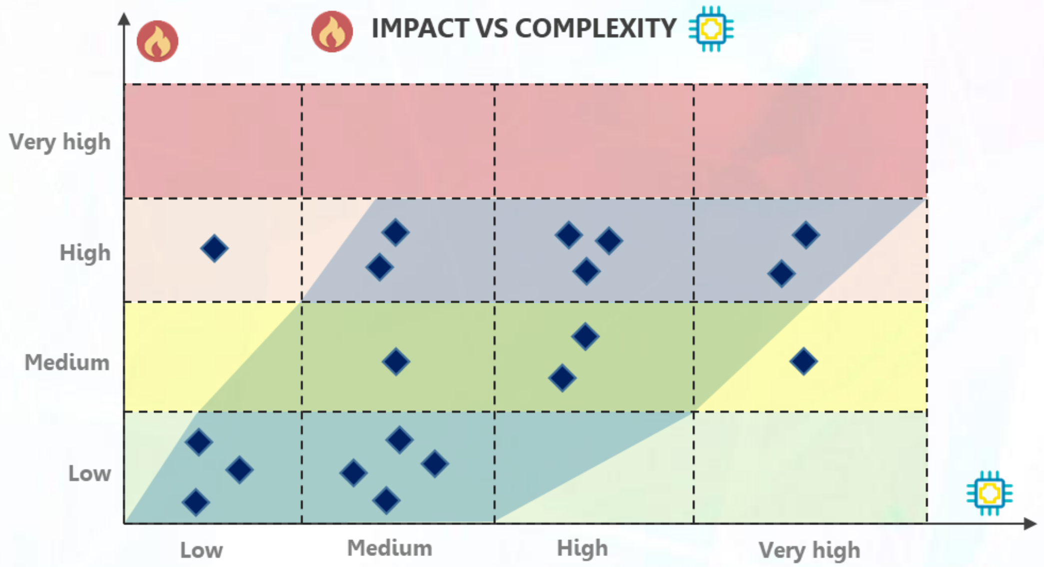
Security has to be set at different layers of a system

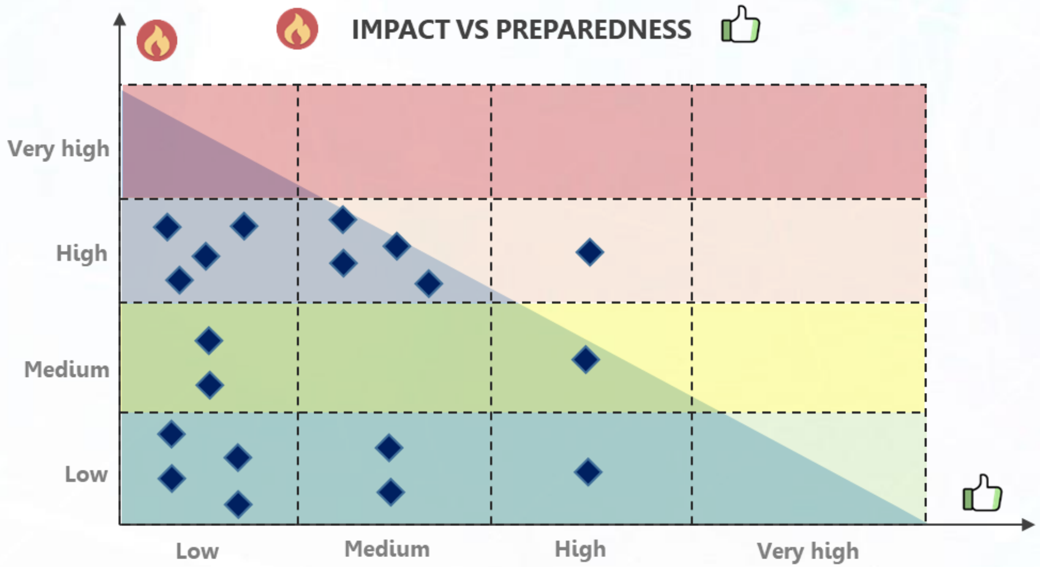
A JEWEL WITH MANY FACTETS

Technical
Legal
Financial
Organizational
Cultural
Regulatory

Cybersecurity is transversal and implies organizations at various levels

Trends from case-studies





Based on case-studies of **19 cyberattacks**
Date: from 2014 to 2019
Victims: Airlines, airports, ANSPs, OEMs, suppliers

Correlation between IMPACT and COMPLEXITY:

- Low but existing correlation
- Low and medium complexity attacks can trigger low, medium or high impact
- High complexity attacks tends to trigger high impact

Need to filter low complexity attacks with basic rules of cyber-hygiene.

Correlation between IMPACT and PREPAREDNESS:

- Strong correlation
- The higher the level of preparedness the lower the impact
- Investments in cybersecurity reduces the level of impact
- Sophistication of cyberattacks is rising…

Investments in cybersecurity are proving to be efficient.

APT groups interested in ANSP's data

Suspected Attribution: Russia
Aka: APT28, Sofacy
Target: **Aerospace**, defense, energy, government, media
Methods: Phishing messages and credential harvesting using spoofed websites.
Registering domains that closely resemble domains of legitimate organizations.

REFINED KITTEN

Suspected Attribution: Iran
Aka: APT33, Elfin, Magnallium, Holmium
Target: Espionage-oriented operations targeting nations and industries (**aerospace**, Defense, Energy, O&G)
Methods: spoofing job postings for defense contractors, decoy job application, first taking an action (e.g. complete a CAPTCHA) that downloads additional PowerShell commands

Suspected Iranian group targeting the **aviation sector** both military and commercial.
Spear-phishing emails recruitment themed lures and contained links to malicious HTML

Suspected Chinese group targeting **aerospace**, and telecom firms, and governments.
Spear phishing and access to victim's networks through managed service providers. spear phishes have been relatively unsophisticated files with double extensions

HELIX KITTEN

Suspected Attribution: Iran
Target: organizations in the **aerospace**, energy, financial, government, hospitality and telecommunications
Methods: thoroughly researched and structured spear-phishing messages, spear-phishing messages sent from compromised accounts of organizations to enhance credibility, backdoor implant, targeting telecommunications can also allow the adversary to be able to reroute communications to adversary-controlled infrastructure

Suspected Chinese group targeting **Aerospace and Defense** and Transportation companies.
Adapted zero-day exploits for operations

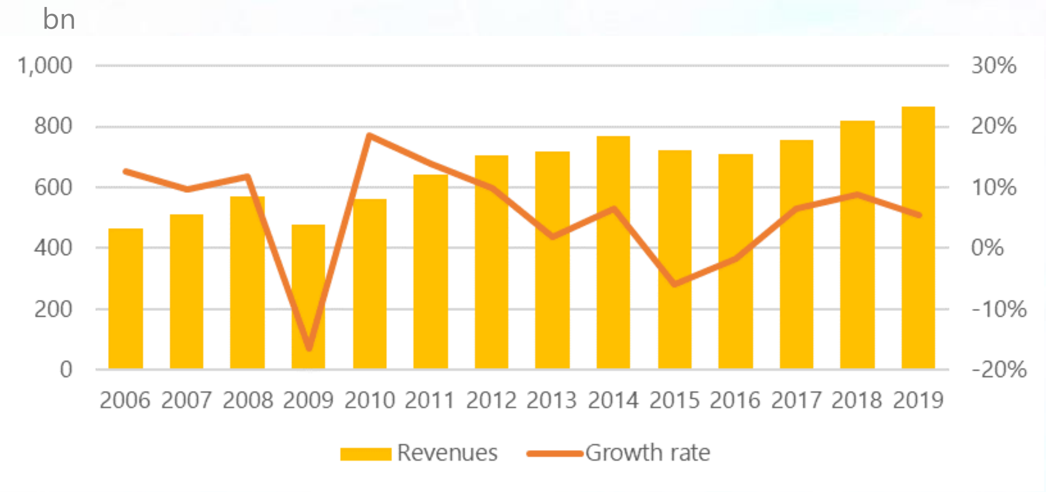
Source Fireeye, crowdstrike

CyberInflight

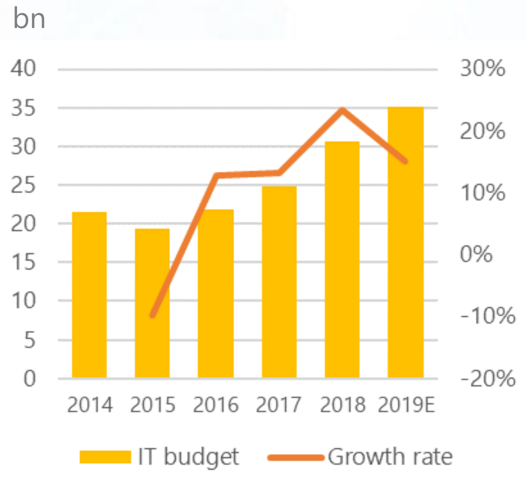
02

Budget oriented approach

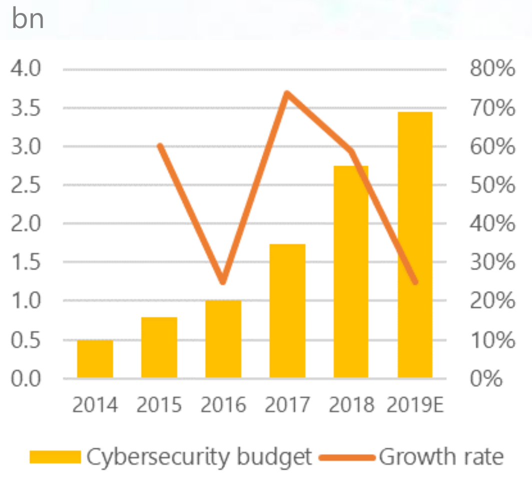
Evolution of airlines cybersecurity budget



IT BUDGET



CYBERSECURITY BUDGET



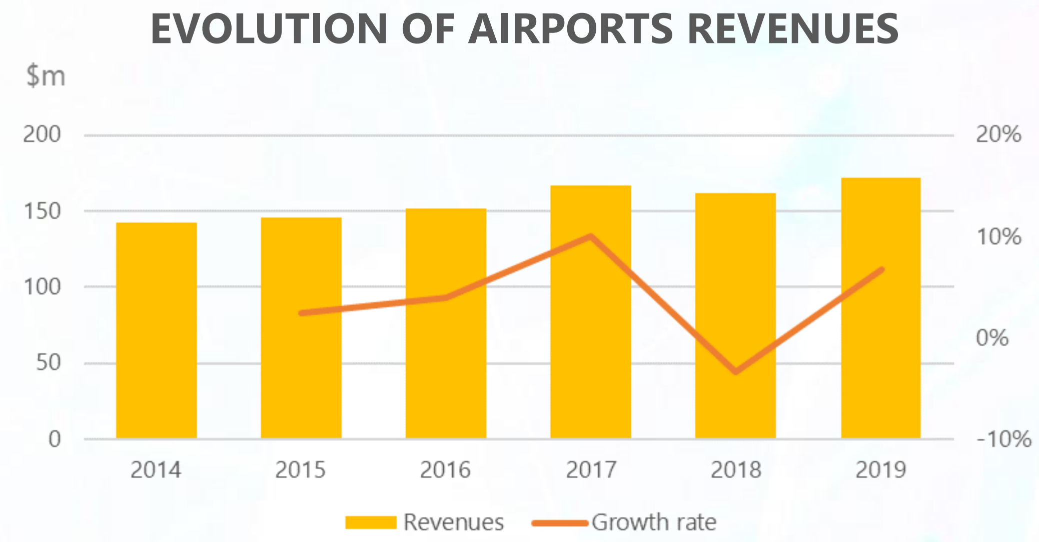
- **Steady** growth of global revenues
- **Significant** growth of IT budget
- **Outstanding** growth of cybersecurity budget

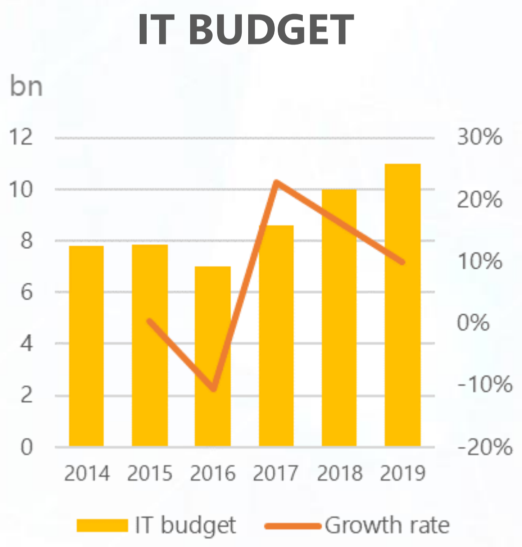
Until the COVID crisis…

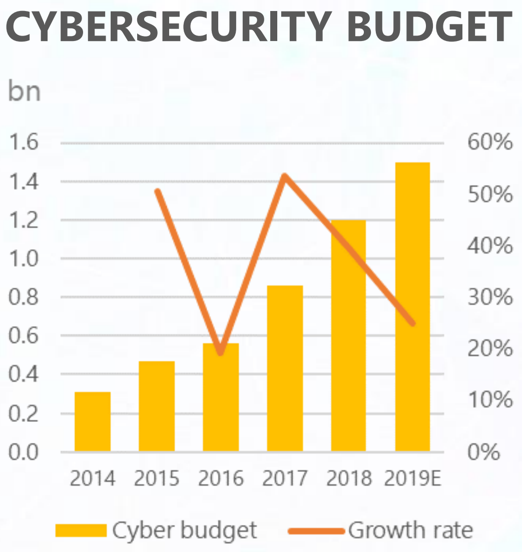
- **Catastrophic** impact on global budget
- IT and cybersecurity budget on hold

Negative impact on companies' cyberdefense mechanisms

Evolution of airports cybersecurity budget





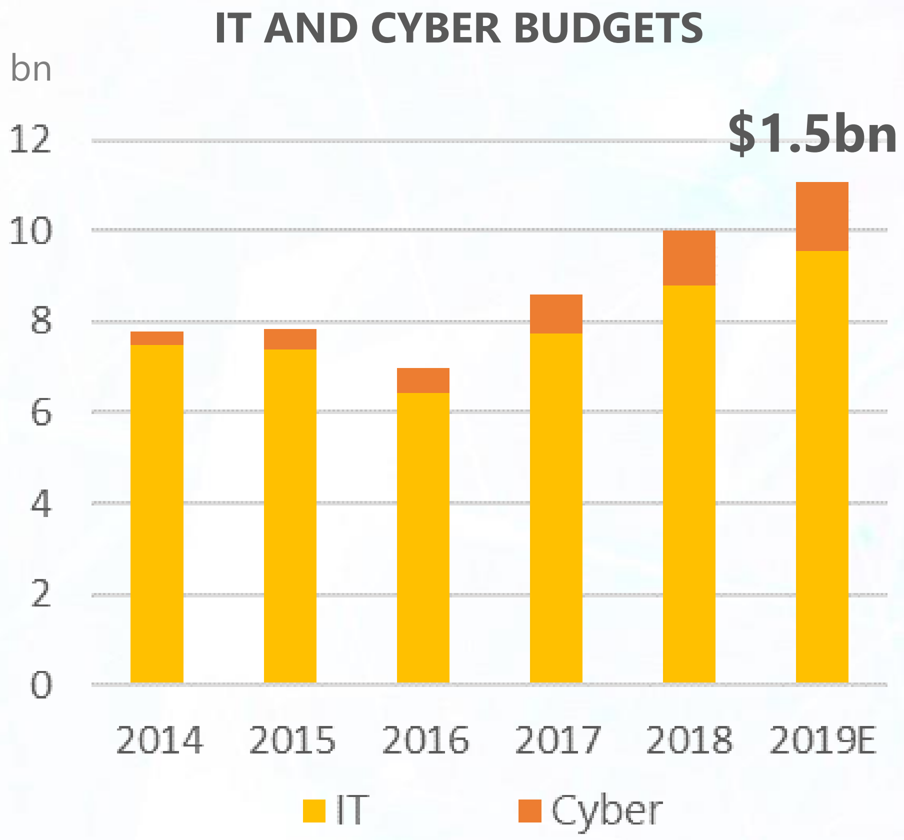


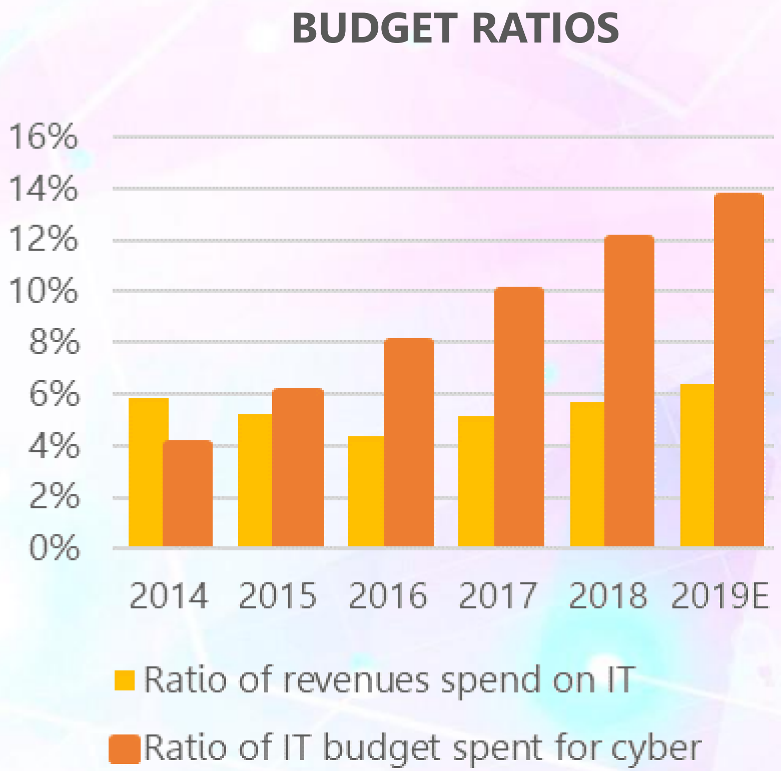
- Airport revenues were more stable over the years than airline revenues

- IT budget has been following a strong growth since 2016
  - Seamless PAX experience
  - Automation

- Cybersecurity budget have followed an outstanding growth rate:
  - **CAGR of 35% since 2014**

Evolution of airports cybersecurity budget

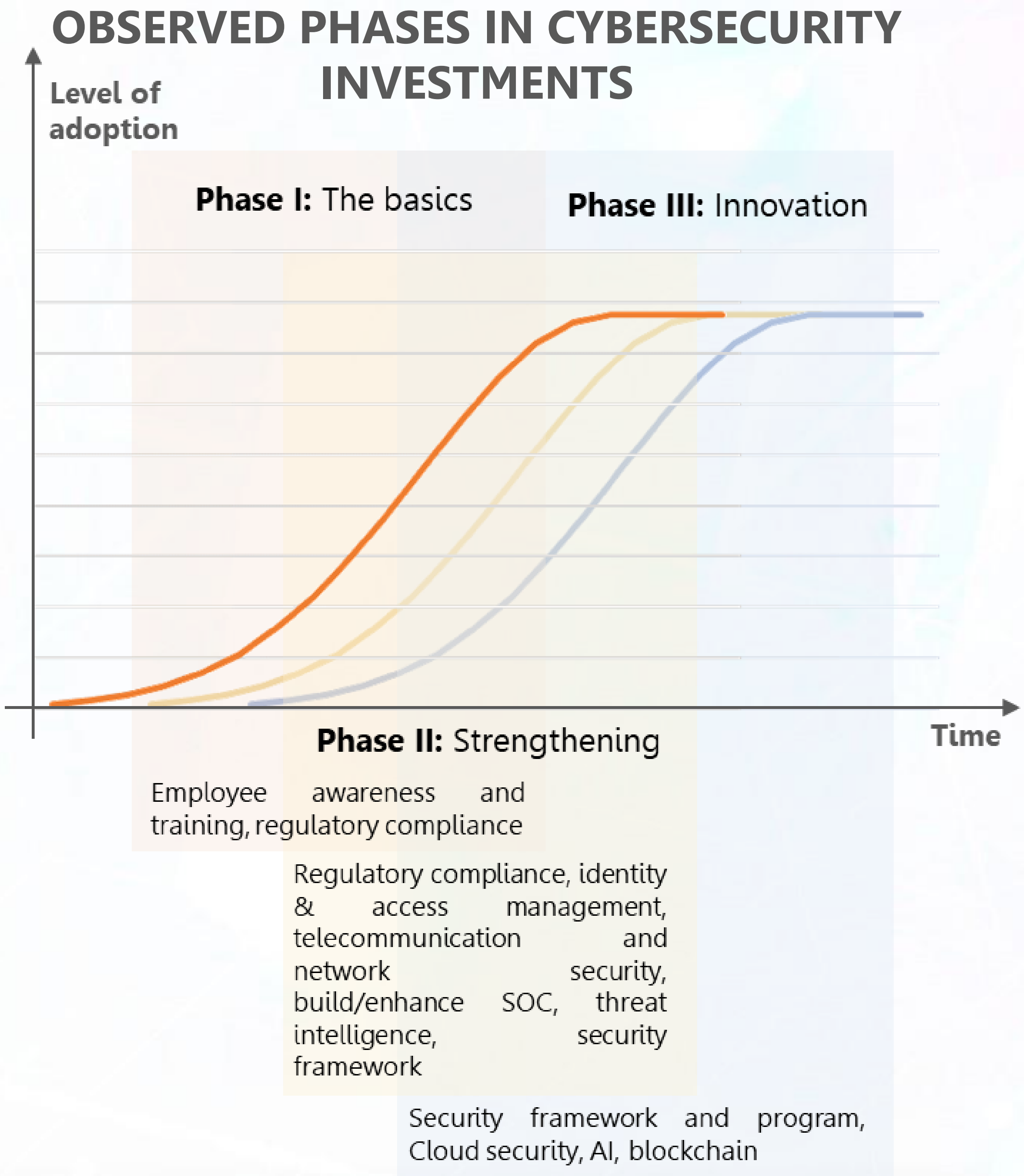




$$\frac{\text{Cyber budget}}{\text{IT budget}}\,\% \qquad \frac{\text{IT budget}}{\text{Total revenues}}\,\%$$

The cyber/IT ratio has reached almost **14% in 2019**
Relatively good level of maturity from airport stakeholders

Phases in cybersecurity investment



- Similar to S-curves applied to cybersecurity investments from basics to consolidation to innovation.

- Different items for cybersecurity investments:

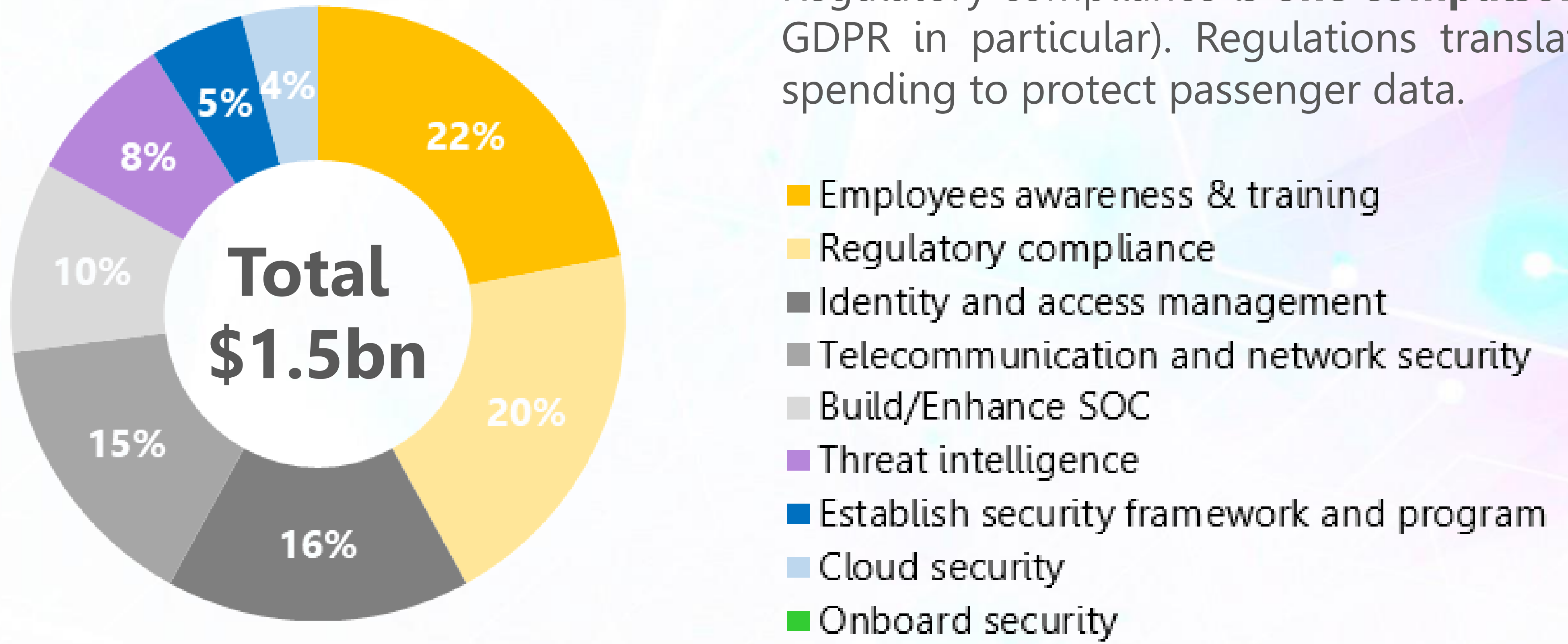
  - Employee awareness and training
  - Regulatory compliance
  - Identity and access management
  - Network security
  - SOC
  - Threat intel.
  - Security framework
  - Cloud security
  - AI, blockchain, innovative technologies…

Cybersecurity budget split for airports

CYBERSECURITY BUDGET SPLIT
(2018 est.)

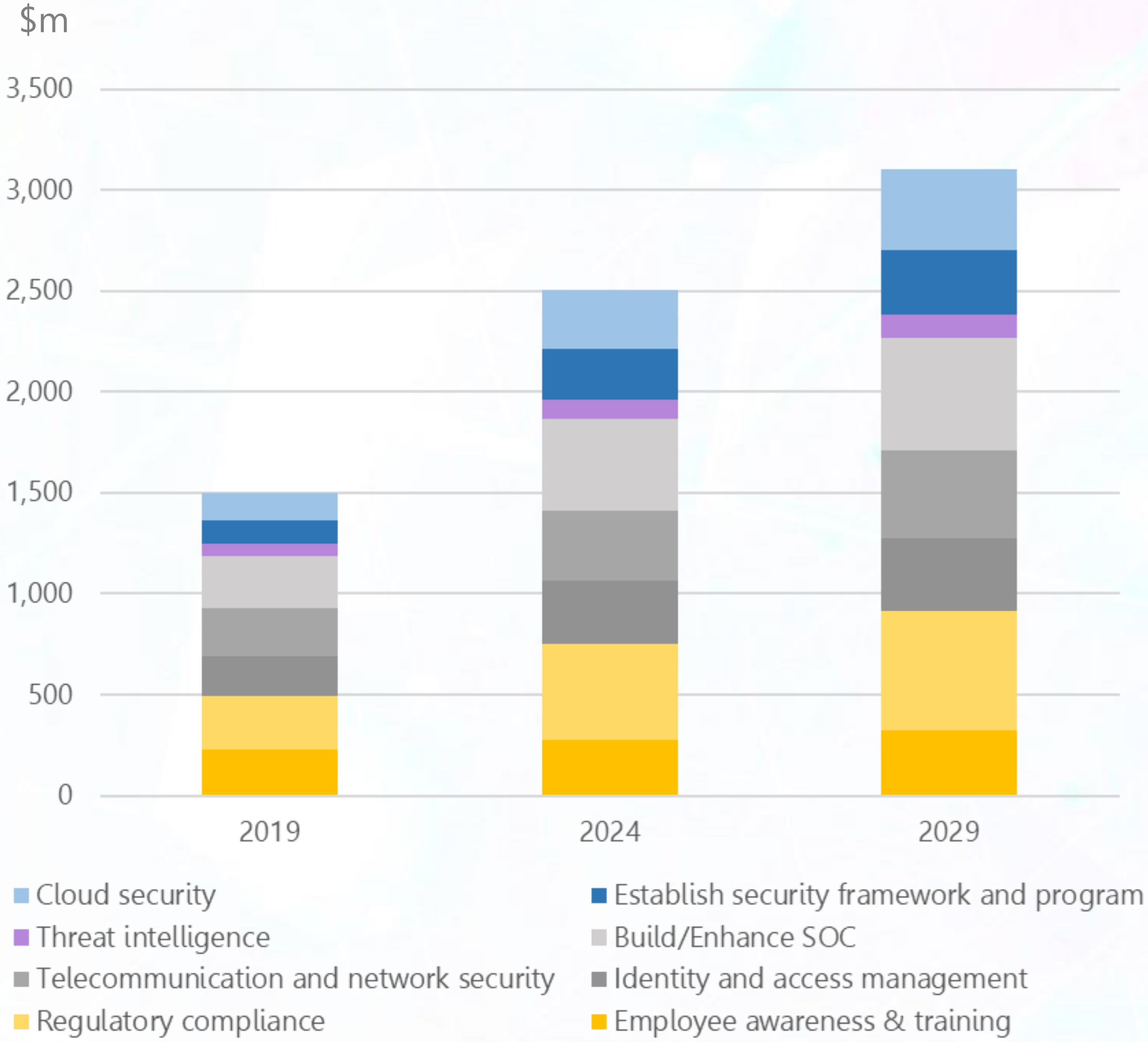
- Airlines have started to seize the importance of **cybersecurity training and awareness**. Rightly the most important item in term of budget.

- Regulatory compliance is **one compulsory investment** (for GDPR in particular). Regulations translates into increased spending to protect passenger data.



Airports’ budget forecast

EVOLUTION OF CYBERSECURITY BUDGET



- Airport cybersecurity spending is poised to grow in the next 10 years from **$1.5bn in 2019 to more than $3.1bn in 2029**, following a 7.6% CAGR
- Cybersecurity already represents 12% of IT budgets in 2019
- Slower increase in cybersecurity budget compare to airline due to **relatively higher maturity**

03

AIDC protocol and data security

AIDC Protocol: ICAO Doc-4444

The AIDC protocol was initially defined in the **9694 Manual released in 1999.**

The AIDC protocol allows to manage a wide range of **key ATM data**

Aircraft related information

Address, ID, type, SSR, COM NAV equipment, etc.

Route related information

ATS route info. , departure info., boundaries info., destination, flight level, distances, position, speed, type of flight, etc.

The AIDC protocol uses **specific message format** and **variable range**

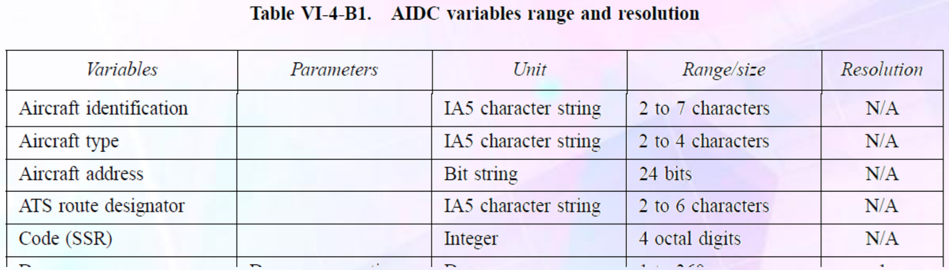
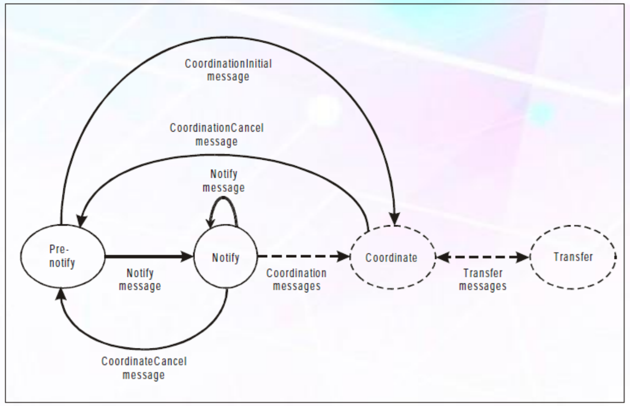


Table VI-4-B1. AIDC variables range and resolution

Variables	*Parameters*	*Unit*	*Range/size*	*Resolution*
Aircraft identification		IA5 character string	2 to 7 characters	N/A
Aircraft type		IA5 character string	2 to 4 characters	N/A
Aircraft address		Bit string	24 bits	N/A
ATS route designator		IA5 character string	2 to 6 characters	N/A
Code (SSR)		Integer	4 octal digits	N/A

The AIDC protocol uses **specific operational sequences and states**



AIDC Protocol: ICAO Doc-4444

“*It is **not the intention that controllers see the messages**, but their operational content is required to be displayed*”

*In order to correctly link a response to an AIDC message with the original message, **a reference to the original message** is included in the response.*

*1.3.3 The message header contains a message **identification**, a **time stamp** (yyyymmddhhmmss) and a **message sequence** number.*

*1.14 **Regional adaptation** of the AIDC application may be accomplished by mutual agreement.*

*1.3.2 An AIDC message is composed of a message header and a sequence of fields of data. Each message shall contain **all the mandatory fields and all relevant optional** fields.*

*1.12 The AIDC application will use the ATN to ensure that ATC data are **exchanged in a reliable** and **timely manner** between ATSUs.*

AIDC Protocol: Ethical hacking approach for AIDC data

First reactions **from an ethical hacking perspective** may trigger the following reaction:

- The protocol was initially defined in 1999. Although the ICAO documents are not related to the implementation of the protocol, there is **no mention to any cybersecurity protection**.
- Operational content of the messages may be visible. A **message modification could hinder the work** of an air traffic controller.
- A hacker could try to **find flaws in AIDC operational sequences of messages** (*ex. of TCP sequence hacking and Man-in-the-middle attack*)
- The implementation of the protocol may be subject to regional adaptation with mutual agreement. This may result in **disparities in the implementation of the protocol** and various level of security.
- Alternative attack could try to attempt to modify timestamps as the AIDC exchanges should happen in a timely manner.
- The use of **optional field is sometimes use by hackers to trigger potential flaws** (*ex. of attacks on the BCBP boarding pass protocol and usage of optional fields*). Is there any checksum or any security related fields?

The current context of cybersecurity threat would require to make sure these questions are answered.

General approach for database security

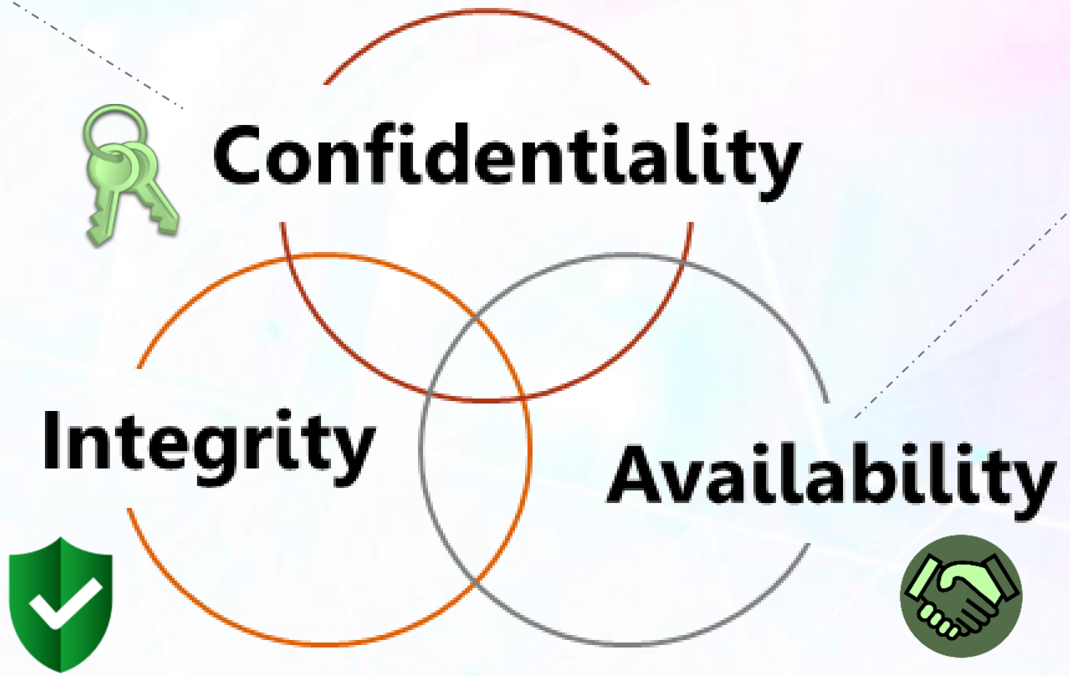
Data security
is based on the **CIA tried**

Only authorized users and processes should be able to access or modify data

Ex. of attack: data breach, leak, exfiltration, espionage, APT, eavesdropping, man-in-the-middle etc.

Data should be maintained in a correct state and nobody should be able to improperly modify it, either accidentally or maliciously

Ex. of attack: interception, manipulation, data compromision, MITM, encryption, ransomware, etc.



Confidentiality

Integrity

Availability

Authorized users should be able to access data whenever they need to do so

Ex. of attack: Denial of Service, DDOS (distributed), protocol sequence attack, NTP attack (timestamp),

Every attack comes down to a loss of one or more of these factors

Cybersecurity basics for databases *(based on national security agency guidelines)*

INFRASTRUCTURE ISOLATION

ATM world is already used to **isolation of sensitive information**. The degree of isolation should be clearly defined. Keep in mind that air-gap networks can still get infected…

Ex #1. of avionics equipment update

Ex #2. ANSP data infected through finance or HR network

Ex #3. Risk link to cloud infrastructure

DATA MAPPING & TAGGING

Identification and categorization of data. A **mapping** allows to have a clear view of your set of data and to know exactly how widely they can be spread. A technical **inventory** of accesses will help to draw potential attack scenarios.

ENCRYPTION

Encryption of data based on a set of parameters: sensitivity, usage, performance, volume, lifetime, spread etc.

Encryption allows **avoiding the publication of confidential data** by ransomware groups on the Dark Web.

Ex. Bombardier, Embraer, ST Engineering etc.

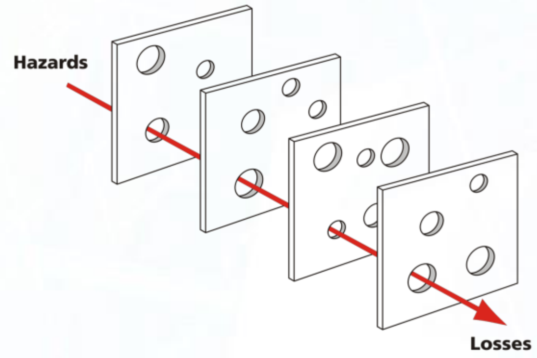
BACKUP & LOGGING

The simplest way to retrieve data encrypted by a ransomware. Frequency and scope of backups to be clearly defined. Efficient logs can allow to detect suspicious activities early.

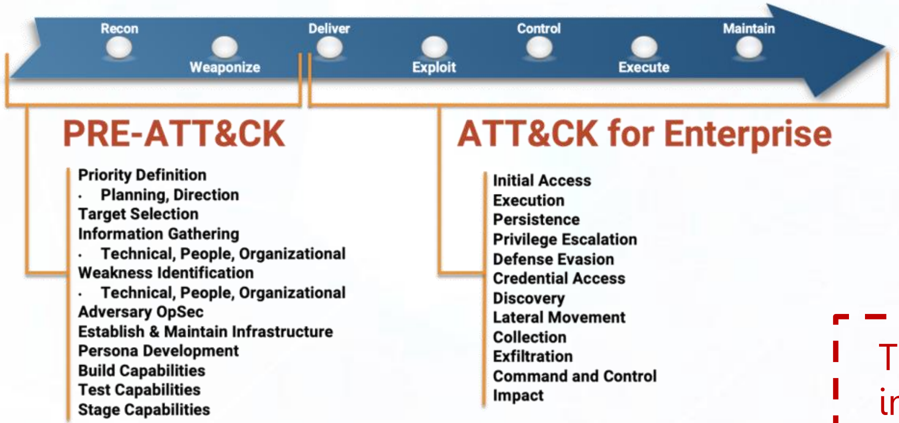
Among other solutions: Authentication, SOC, SIEM, threat intelligence, regulatory compliance, awareness & training, cloud security, AI, etc.

Defense Frameworks & Key Resources (1/2)

Swiss Cheese Model



MITRE Framework



PRE-ATT&CK

Priority Definition
- Planning, Direction

Target Selection
Information Gathering
- Technical, People, Organizational

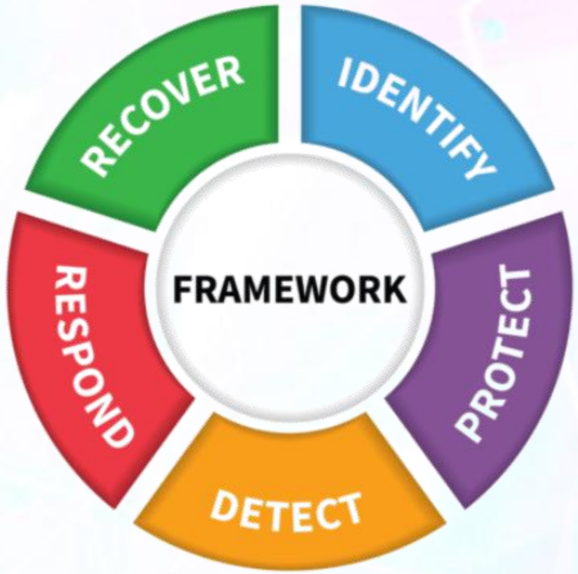
Weakness Identification
- Technical, People, Organizational

Adversary OpSec
Establish & Maintain Infrastructure
Persona Development
Build Capabilities
Test Capabilities
Stage Capabilities

ATT&CK for Enterprise

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control
Impact

NIST Framework



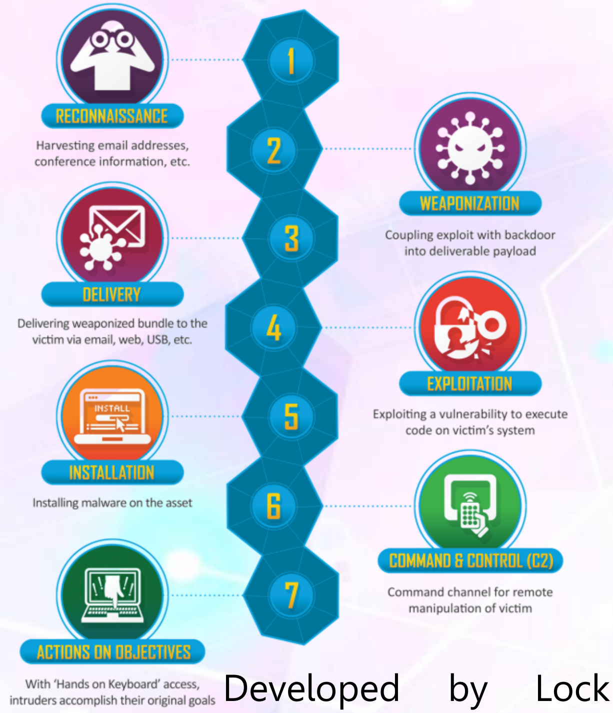
Frameworks for voluntary use, can be used by organizations in **any sector or community** regardless of size, degree of risk or sophistication

To apply the **principles and best practices of risk management**

The NIST framework has been implemented by CANSO (cf. Cyber Security and Risk Assessment Guide)

canso
civil air navigation services organisation

Cyber Kill Chain

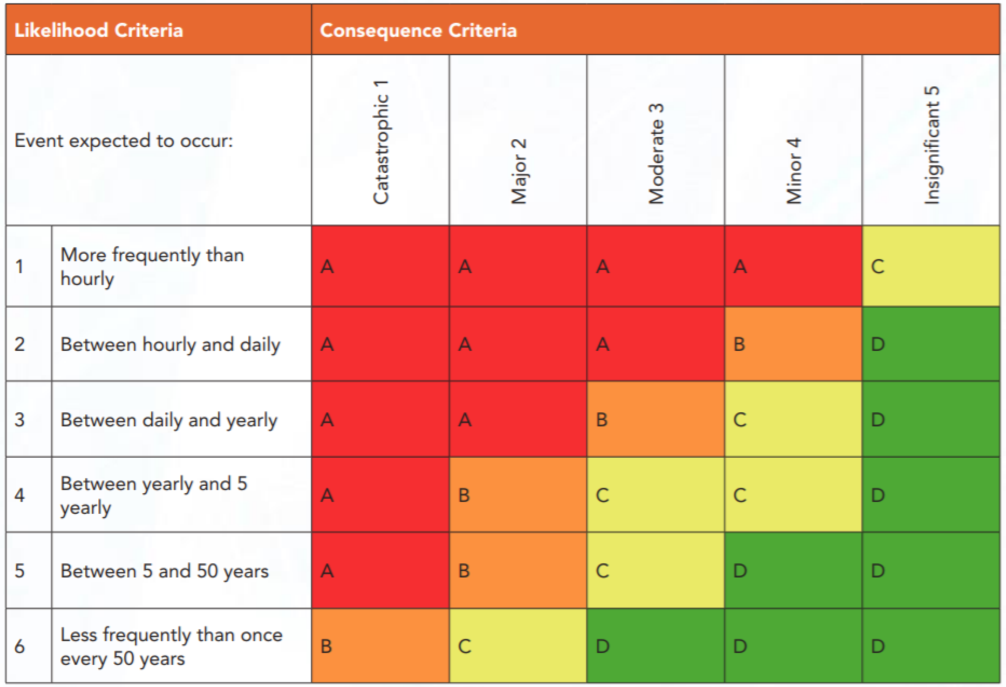

1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Developed by Lockheed Martin, **the Cyber Kill Chain®** framework is used to identify and prevent cyber intrusion activities.

Defense Frameworks & Key Resources (2/2)

EXAMPLE OF CANSO CYBER SECURITY AND RISK ASSESSMENT GUIDE

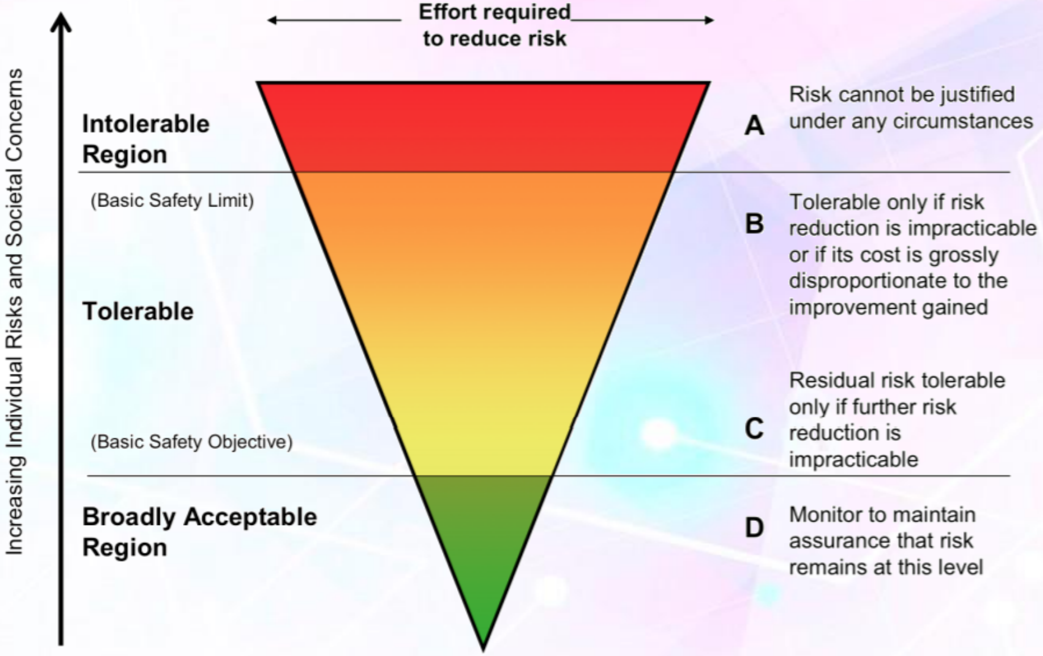
Consequence VS Likelihood



Likelihood Criteria		Consequence Criteria				
Event expected to occur:		Catastrophic 1	Major 2	Moderate 3	Minor 4	Insignificant 5
1	More frequently than hourly	A	A	A	A	C
2	Between hourly and daily	A	A	A	B	D
3	Between daily and yearly	A	A	B	C	D
4	Between yearly and 5 yearly	A	B	C	C	D
5	Between 5 and 50 years	A	B	C	D	D
6	Less frequently than once every 50 years	B	C	D	D	D

The conversion of the combination of consequence and likelihood into a risk rating has been achieved by use of the following matrix.

Consequence VS Effort required to reduce risk



Effort required to reduce risk
Increasing Individual Risks and Societal Concerns
Intolerable Region
(Basic Safety Limit)
Tolerable
(Basic Safety Objective)
Broadly Acceptable Region
A
Risk cannot be justified under any circumstances
B
Tolerable only if risk reduction is impracticable or if its cost is grossly disproportionate to the improvement gained
C
Residual risk tolerable only if further risk reduction is impracticable
D
Monitor to maintain assurance that risk remains at this level

Perspective of the timeliness of the corrective action required.

Source CANSO

canso

CANSO Standard of Excellence in Cybersecurity

A recently published guideline is the **CANSO standard of Excellence in Cybersecurity** report

05

Takeaways

Hats off to ICAO's effort in cybersecurity

ICAO CYBERSECURITY INITIATIVES

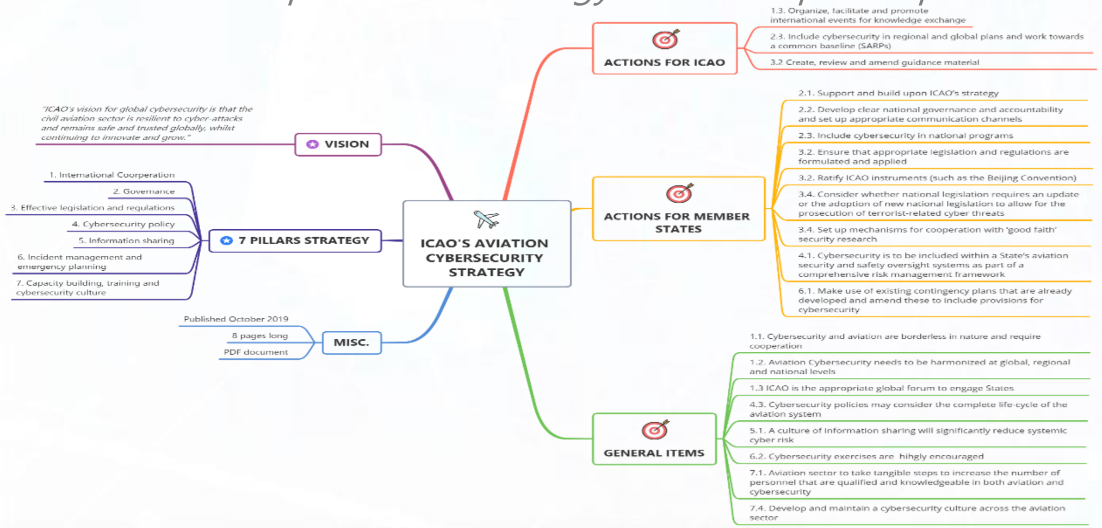
Aviation Cybersecurity strategy

Bucharest communique

Declaration on cybersecurity in civil aviation

ICAO Resolution A39-19

Mindmap of ICAO's strategy available upon request



ICAO'S AVIATION CYBERSECURITY STRATEGY

VISION

"ICAO's vision for global cybersecurity is that the civil aviation sector is resilient to cyber-attacks and remains safe and trusted globally, whilst continuing to innovate and grow."

7 PILLARS STRATEGY

1. International Coorperation
2. Governance
3. Effective legislation and regulations
4. Cybersecurity policy
5. Information sharing
6. Incident management and emergency planning
7. Capacity building, training and cybersecurity culture

MISC.

Published October 2019

8 pages long

PDF document

ACTIONS FOR ICAO

1.3. Organize, facilitate and promote international events for knowledge exchange

2.3. Include cybersecurity in regional and global plans and work towards a common baseline (SARPs)

3.2 Create, review and amend guidance material

ACTIONS FOR MEMBER STATES

2.1. Support and build upon ICAO's strategy

2.2. Develop clear national governance and accountability and set up appropriate communication channels

2.3. Include cybersecurity in national programs

3.2. Ensure that appropriate legislation and regulations are formulated and applied

3.2. Ratify ICAO instruments (such as the Beijing Convention)

3.4. Consider whether national legislation requires an update or the adoption of new national legislation to allow for the prosecution of terrorist-related cyber threats

3.4. Set up mechanisms for cooperation with 'good faith' security research

4.1. Cybersecurity is to be included within a State's aviation security and safety oversight systems as part of a comprehensive risk management framework

6.1. Make use of existing contingency plans that are already developed and amend these to include provisions for cybersecurity

GENERAL ITEMS

1.1. Cybersecurity and aviation are borderless in nature and require cooperation

1.2. Aviation Cybersecurity needs to be harmonized at global, regional and national levels

1.3 ICAO is the appropriate global forum to engage States

4.3. Cybersecurity policies may consider the complete life-cycle of the aviation system

5.1. A culture of information sharing will significantly reduce systemic cyber risk

6.2. Cybersecurity exercises are hihgly encouraged

7.1. Aviation sector to take tangible steps to increase the number of personnel that are qualified and knowledgeable in both aviation and cybersecurity

7.4. Develop and maintain a cybersecurity culture across the aviation sector

According to ICAO:

- SARPS and guidance materials (Doc 8973) are considered high-level and there is an **urgent need for more specific guidance** that can be applied by States
- Cybersecurity is a topic that should be included in the security culture through **the training delivered to the staff** of the air transport ecosystem
- The **establishment of a global trust framework would definitely improve safety and resilience** of air traffic management and aircraft operations

With the A40-10 resolution, ICAO has taken one of the **most significant step toward a cybersecure airspace.**

Information sharing remains key

AVIATION ISAC

ICAO · OACI · ИКАО

FIRST

CERT-EU

canso
civil air navigation services organisation

EUROCONTROL

CISA

AIRPORTS COUNCIL INTERNATIONAL

IATA

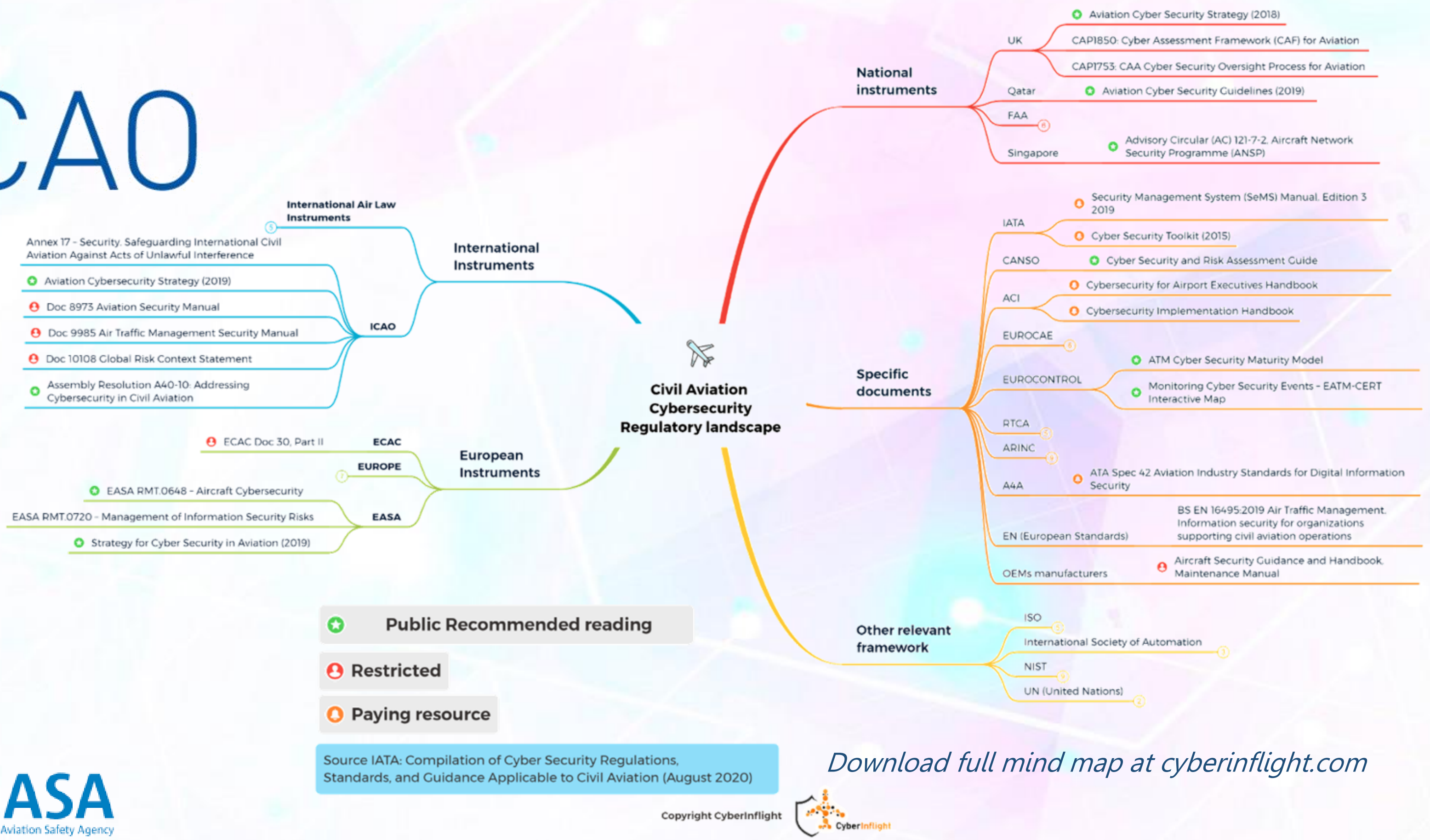
CISA

GCHQ

Bundesamt
für Sicherheit in der
Informationstechnik

EUROCONTROL

EASA
European Union Aviation Safety Agency



Civil Aviation Cybersecurity Regulatory landscape

International Instruments
- International Air Law Instruments
- ICAO
  - Annex 17 - Security. Safeguarding International Civil Aviation Against Acts of Unlawful Interference
  - ● Aviation Cybersecurity Strategy (2019)
  - ● Doc 8973 Aviation Security Manual
  - ● Doc 9985 Air Traffic Management Security Manual
  - ● Doc 10108 Global Risk Context Statement
  - ● Assembly Resolution A40-10: Addressing Cybersecurity in Civil Aviation

European Instruments
- ECAC
  - ● ECAC Doc 30, Part II
- EUROPE
- EASA
  - ● EASA RMT.0648 - Aircraft Cybersecurity
  - EASA RMT.0720 - Management of Information Security Risks
  - ● Strategy for Cyber Security in Aviation (2019)

National instruments
- UK
  - ● Aviation Cyber Security Strategy (2018)
  - CAP1850: Cyber Assessment Framework (CAF) for Aviation
  - CAP1753: CAA Cyber Security Oversight Process for Aviation
- Qatar
  - ● Aviation Cyber Security Guidelines (2019)
- FAA
- Singapore
  - ● Advisory Circular (AC) 121-7-2. Aircraft Network Security Programme (ANSP)

Specific documents
- IATA
  - ● Security Management System (SeMS) Manual. Edition 3 2019
  - ● Cyber Security Toolkit (2015)
- CANSO
  - ● Cyber Security and Risk Assessment Guide
- ACI
  - ● Cybersecurity for Airport Executives Handbook
  - ● Cybersecurity Implementation Handbook
- EUROCAE
- EUROCONTROL
  - ● ATM Cyber Security Maturity Model
  - ● Monitoring Cyber Security Events - EATM-CERT Interactive Map
- RTCA
- ARINC
- A4A
  - ● ATA Spec 42 Aviation Industry Standards for Digital Information Security
- EN (European Standards)
  - BS EN 16495:2019 Air Traffic Management. Information security for organizations supporting civil aviation operations
- OEMs manufacturers
  - ● Aircraft Security Guidance and Handbook. Maintenance Manual

Other relevant framework
- ISO
- International Society of Automation
- NIST
- UN (United Nations)

● Public Recommended reading

● Restricted

● Paying resource

Source IATA: Compilation of Cyber Security Regulations, Standards, and Guidance Applicable to Civil Aviation (August 2020)

Download full mind map at cyberinflight.com

CyberInflight

Qatar CAA

الهيئة العامة للطيران المدني
CIVIL AVIATION AUTHORITY

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Munich Airport

ISH
Information Security Hub

Airport Council

AIRPORTS COUNCIL INTERNATIONAL
EUROPE

CCTA (by French DGAC)

14 CCTA MEMBERS

STATE ACTORS	INDUSTRY PLAYERS	ORGANIZATIONS/FEDERATIONS
ANSSI	AIRBUS	**GIFAS**: Groupement des Industries Francaises Aéronautiques et Spatiales (Association of the French Aerospace industry)
Interior Ministry	THALES	**FNAM**: Fédération Nationale de L'aviation marchande (National Federation for Commercial Aviation)
Army Ministry	DASSAULT AVIATION	**UAF**: Union des Aéroports Français (French Airports Association)
Transport Ministry	SAFRAN	
DGAC/DSNA	ADP	
	Air France	

DEFCON Aerospace Village

AEROSPACE VILLAGE

CyberInflight: How can we help you ?

Awareness & training on aerospace cybersecurity

Customized training for your staff

Threat intelligence with aerospace case studies

Agenda

SESSION 1: ASSESS THE THREAT

1 | Introduction
Digitization
Technology Adoption

2 | Cybercrime economy
Hacker's methodology

3 | Case studies, examples & screenshots

4 | Wrap-up & Takeaways

SESSION 2: DEFEND FORWARD

1 | Market Overview, Analysis
Forecast

2 | Cyber hygiene
Organizational processes

3 | Regulatory framework
Cyber-insurance

4 | Takeaways &
Final conclusion

Copyright CyberInflight

4

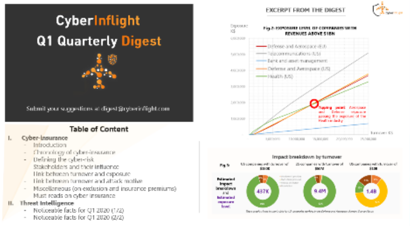
Our Quarterly Digest Subscription

Aerospace cybersecurity news

Submit your topic of interest

Get already published digests:

cyber-insurance, dark web, regulatory landscape, retrospective of the year 2020



CyberInflight
Q1 Quarterly Digest

Submit your suggestions at digest@cyberinflight.com

Table of Content

I. Cyber-Insurance
- Introduction
- Chronology of cyber-insurance
- Defining the cyber-risk
  Stakeholders and their influence
  Link between turnover and exposure
- Link between turnover and attack motive
- Miscellaneous (on exclusion and insurance premiums)
  Must reads on cyber insurance

II. Threat Intelligence
- Noticeable facts for Q1 2020 (1/2)
- Noticeable facts for Q1 2020 (2/2)

EXCERPT FROM THE DIGEST

Fig 2: EXPOSURE LEVEL OF COMPANIES WITH REVENUES ABOVE $1BN
Exposure K$
Defense and Aerospace (EU)
Telecommunications (US)
Bank and asset management
Defense and Aerospace (US)
Health (US)
Turnover K$
Impact breakdown by turnover
437K
9.4M
1.4B

Our flagship strategic report

Aerospace Cybersecurity Market Intelligence report, Edition 2020

Highly infographic and data oriented

127 pages

Aerospace Cybersecurity

Market Intelligence Report

1st Edition
Published: January 2020
Copyright © 2020 CyberInflight
All rights reserved.

Sector trends and dynamics, analysis and forecast addressing the Aerospace Cybersecurity market

- Market outlook
- Sector trends and dynamics
- Strategic analysis and forecast
- Stakeholders' profile
- Regulatory landscape
- Threat intelligence

www.cyberinflight.com

Consulting & Strategic Advisory

- **Strategic partnership**
- **Support to the CISO on cyber-strategy**
- **Build communication supports** for decision-makers
- **Market analysis** of key topics and future trends
- **Go-to-market strategies** analysis
- **Benchmarking** of cybersecurity product
- Interview campaigns, peers, identification of subject matter experts

Would you be interested in a strategic report dedicated to the ATM ecosystem ?

Topics tackled: trends, technology, budget, regulations, standards, insurance, threat intelligence, good practices, recommendations, geographical views & opinions etc.

contact me at florent.rizzo@cyberinflight.com