THE CYBER AIRPORT

A PRACTICAL GUIDE FOR AIRPORT EXECUTIVES

OVERVIEW
SPECIFIC RISKS
PRACTICAL INFORMATION

UAF&FA
UNION DES AÉROPORTS FRANÇAIS & FRANCOPHONES ASSOCIÉS

THE CYBER AIRPORT

A PRACTICAL GUIDE FOR AIRPORT EXECUTIVES

OVERVIEW
SPECIFIC RISKS
PRACTICAL INFORMATION

Guide compiled from the collective work of airports affiliated to the IT Commission of the Union des Aéroports Français et Francophones Associés (UAF & FA),
the French and French-speaking airports association

Thomas JUIN
Chairman of the Union des Aéroports
Français & Francophones Associés
the French and French-speaking Airports Association

Laurent VERBIGUIÉ
Chairman of the
IT Commission and Innovation Group

EDITORIAL

Cybersecurity is a critical and inevitable concern for everyone. However, it shouldn't be considered as purely a constraint: it is also an opportunity to **maintain business continuity as a source of both added value and productivity.** Yet, the subject remains difficult to grasp for any neophytes who often imagine analyses that are too technical and complex.

This document draws on our experience gained through talking with airport executive bodies and aeronautical experts; its purpose is to make airport cybersecurity easy to fathom and understand.

You will find key information on the current landscape (risks, regulations, etc.) and practical recommendations to tackle the various threats faced by your organisation: those linked to man and those linked to technology...

Cybersecurity requires a long-term commitment. This Practical Guide will enable you to familiarize yourself with the issues and provide food for thought going forward.

Happy and instructive reading!

Éric VAUTIER
Chief Information Security Officer
(CISO)

CISO EDITORIAL

A position with profiles and assignments that vary from one organisation to another, Chief Information Security Officers (CISO) have seen their responsibilities develop dramatically in a very short period of time. In less than ten years, **Cybersecurity has evolved from a technical matter to a major preoccupation for company directors,** without the CISO necessarily seeing human and financial resources increase accordingly.

The notion of community takes on its full meaning and force under such circumstances. The CISO community of the French-speaking Airports Association formed naturally within the IT Commission of the AFACI back in 2013. Since then, the Cybersecurity Working Group has provided support and recommendations not only to the French National Cybersecurity Agency [ANSSI] within the framework of the Critical Infrastructure Information Protection law (CIIP law), but also to the work of the Ministry for Ecological and Solidarity Transition with regards to cybersecurity and has, of course, produced specific deliverables for the airport sector.

This guide represents the latest deliverable of the Working Group: a delicate exercise in raising awareness, spreading the word and demystifying. We hope that reading it will enable you to better understand the broad range of tasks carried out by your CISO.

Editorial management:
Laurent Verbiguié

Editorial college:
Éric Vautier, Jean-Luc Martin, Kévin Alet

Texts:
Nostromo (Jean-Marie Benoist, Guillaume Wallut)

Graphic design and layout:
Justine Torres

Coordination:
Justine Torres

Printing and finishings:
Stipa, Montreuil

Edition:
2018

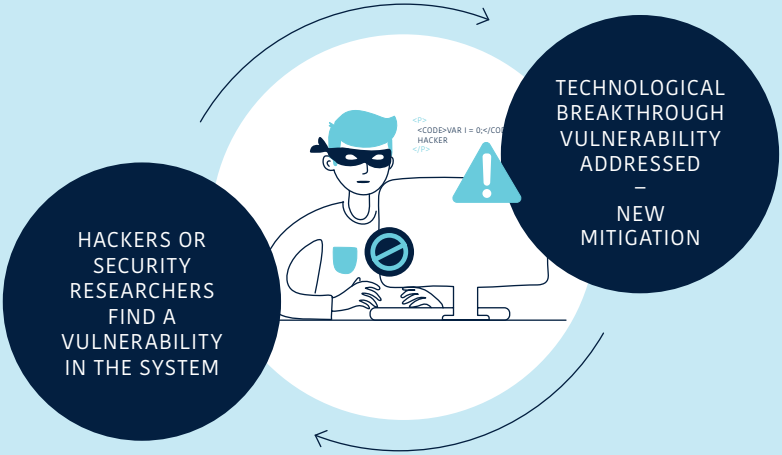
English translation:
2019

TABLE OF CONTENTS

PART 1

OVERVIEW

THE CYCLES


HACKERS OR SECURITY RESEARCHERS FIND A VULNERABILITY IN THE SYSTEM
TECHNOLOGICAL BREAKTHROUGH VULNERABILITY ADDRESSED – NEW MITIGATION
HACKER


SERVICES (CUSTOMERS, EMPLOYEES, PARTNERS)
BEST PRACTICES
COMMUNICATION
VIGILANCE
RISK MANAGEMENT

THE DIGITAL PARADOX

On the one hand, customers, employees, partners and the company need increasingly **open, flexible and connected digital services.** On the other hand, **any connection between two devices, networks or software programs inevitably introduces risks** that must be guarded against. How can access be controlled and opened up at the same time, and how can this be achieved over the long term?

The cybersecurity challenge lies in amalgamating these two contradictory positions. Ignoring the issue is not an option: cybersecurity is an obvious imperative. Just as it would be out of the question to buy a car without airbags, safety belts and insurance, it is also out of the question to offer or use digital services and tools without having assessed the risks and implemented the necessary protective measures. The solution: **explicit cooperation between the stakeholders.** Services offered must be secure and come with a set of best practices that are clearly explained to users, who adhere to these best practices and report any disorderly or inappropriate aspects without waiting for an incident to occur.

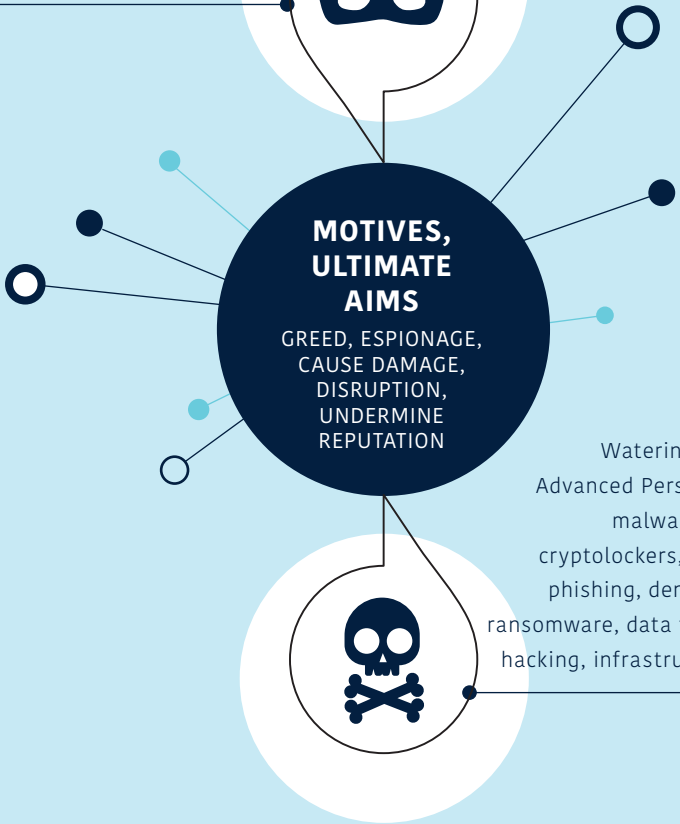
THE SOLUTION: EXPLICIT COOPERATION BETWEEN THE STAKEHOLDERS

This Guide will provide you with the essential elements to begin or perfect your cybersecurity process.

TYPES OF ATTACK AND MOTIVES

ATTACKERS

Intentional (or unintentional) insiders, business competitors, criminal organisations, terrorists, hacktivists, States



ATTACKS

Watering hole attack, Advanced Persistent Threat, malwares, sabotage, cryptolockers, malvertising, phishing, denial of service, ransomware, data theft, website hacking, infrastructure hacking

DIGITAL WARFARE

CYBERCRIME WILL COST OVER 2,000 BILLION DOLLARS IN 2019

Let there be no mistake, digital war is already raging. An increasing number of attacks are hitting the headlines, and those that we don't hear about are growing exponentially. **Cybercrime will cost over 2,000 billion dollars in 2019** – four times more than in 2015, and in 2020, the average cost of a data breach will exceed 150 million dollars*. But the consequences of an attack are not only financial; there is also loss of customers' trust, damage to reputation and client safety... The growing interdependence between analogue electronics and digital worlds exacerbates the consequences of an attack.

The most frequent motive is financial: ransomware attacks increased by 36% in 2017**. However, this is only one aspect of the threats faced by companies and even now purely destructive attacks occur. The most worrying part is the lack of awareness with regard to the scale of what is at stake. On average, **a company takes over 190 days to realise that it has been hacked*****... This indeed paints a dismal picture and it is urgent to take action.

* Source: Juniper Research ** Source: Symantec *** Source: Ponemon Institute

BANKING REGULATIONS

New obligations relating to cybersecurity increasingly means ensuring that a **company's partners are also in compliance with regard to their obligations.** It is, therefore, necessary to know not only what applies to one's own company, but also what applies to others.

Among the different business sectors, **the realm of payment is becoming increasingly regulated.** Its stakeholders must abide by the PSD2 European Directive, which came into effect in January 2018.

It imposes new security regulations: secure exchanges between applications, strong authentication, etc. but also opens the way to new services: information aggregation, payment initiation, etc.

FOR NOW, HALF OF THE ESTABLISHMENTS CONCERNED ARE NOT YET READY*

* Source : Finextra

In addition, the SWIFT bank system **has compelled all members of its network to adopt new security standards:** secure environment, controlled and limited access, incident detection and response... A situation report must be published annually by each member.

DATA PROTECTION AND CIVIL LIBERTIES 2.0

The General Data Protection Regulation (GDPR) is a European regulation that is fully in keeping with the French Data Protection Act. It came into effect on 25th May 2018 and has three objectives: **create confidence, make stakeholders accountable and ensure greater legal protection for the collection of personal data.**

From now on, companies are responsible for the data they process (even via a service provider) and are subject to **an obligation to provide evidence of their actions.** New rights for employees and customers have also been established: the right of portability and deletion of data, systematically seeking consent when gathering personal data, etc.

NEW CUSTOMER AND EMPLOYEE RIGHTS HAVE BEEN ESTABLISHED

Finally, the regulation strengthens data security, moving from an obligation of means to an **obligation of result.** In order to facilitate monitoring, the GDPR recommends the creation of a new position, the **Data Protection Officer (DPO),** in charge of correctly processing data within the company. To find out more, read pages 32 to 33.

EUROPEAN NIS DIRECTIVE

The European Directive on Security of Network and Information Systems (NIS), adopted in July 2016, was transposed into European Member States.

Apart from nationwide obligations: setting up a cybersecurity strategy, an authority in charge of these matters, etc., it introduced new obligations for two types of stakeholder: Operators of essential services (OES), with regards to numerous business sectors including air transport, and Digital Service Providers (DSPs), covering a large number of such service providers.

THE OBLIGATIONS OF THESE STAKEHOLDERS ARE MORE OR LESS SIMILAR:

- **Take the necessary technical and organisational measures,** proportionate and adjusted to the management of risks threatening the security of networks and information systems;
- **Take appropriate measures to prevent incidents** that compromise the security of networks and information systems;
- **Send notification (to the European State National appropriate competent authority (e.g. according to the French National Cybersecurity Agency - ANSSI)),** without undue delay, of any incident that has a significant impact on the continuity of essential services, as soon as they become aware of it.

The security rules necessary for the protection of networks and information systems are laid down, in France, by the Prime Minister, and may be updated to take into account the state of knowledge. **French transposition of the NIS Directive stipulates four areas of obligation:**

- Governance of networks and information system security;
- Protection of networks and information systems;
- Defence of networks and information systems;
- Resilience of activities.

The Directive also provides for severe penalties in the form of fines should any obligations fail to be met.

	OES	DSP
non-compliance with security obligations	€100,000	€75,000
failure to declare an incident	€75,000	€50,000
impeding operations	€125,000	€100,000

NEWS IN BRIEF

and the world of aeronautics in general have long been the target of choice for cyber-attacks.

2011 Los Angeles airports (LAX, ONT, VNY and PMD) have blocked nearly 60,000 cases of improper use of Internet and 2.9 million hacking attempts in just one year.

2013 An Advanced Persistent Threat from a sophisticated group of hackers acting for a State used a reliable industry source to send phishing emails to airports: 75 airports were affected, 2 had their systems compromised.

2013 Miami International Airport (MIA) was subjected to nearly 200,000 hacking attempts per day before investing in training, education and new technology to protect itself from cyberattacks.

2014 The Indian Airport Authority's enterprise resource planning system was successfully hacked, which made the system inoperative and, above all, led to the leakage of employees' personal data.

2016 According to the European Aviation Safety Agency, aviation systems are subjected to over 1,000 attacks per month.

2016 The night following the Brussels Airport terrorist attack on the 22 March 2016, an American teenager living in Pittsburgh attacked the Brussels Airport company website with declared aim of infiltrating their information system.

2017 Several massive ransomware attacks (WannaCry, GoldenEye, BadRabbits...) affected, among other victims, the airports of Ukraine, especially Boryspil in Kiev (KBP) and Odessa (ODS).

SOME KEY TECHNOLOGIES

Technology is not the universal remedy for all problems, but it is an indispensable ingredient that supports strategies and action plans, as long as the users are aware and trained. **Three solutions are particularly to be taken into consideration.**

STRONG AUTHENTICATION

Despite all the recommendations given: single password per account, varying characters and case, etc., the single password is still a risk. Today, double authentication solutions are varied: smart cards, sms, etc., and are well integrated in private practice, which makes their adoption in the corporate setting much easier.

BIG DATA

Cybersecurity produces and consumes a large amount of data: monitoring threats, auditing logs, predicting attacks, etc. Big Data is one of the solutions to efficiently handle and process such a large volume of information.

CLOUD AND SAAS (Software As A Service)

As for many other digital applications, cybersecurity solutions benefit from the contribution of the Cloud and SaaS mode solutions, especially in terms of access, cost, storage and processing of data. However, consideration must be given to solutions “in the Cloud”, as this brings new risks that must be controlled.

PART 2

AIRPORTS

MULTIPLE SOURCES OF RISK

When moving through an airport, a passenger comes into direct and indirect contact with various technologies and sensitive data. Following the passenger journey provides a first inventory of all the subjects to analyse when assessing the threats faced by the airport.

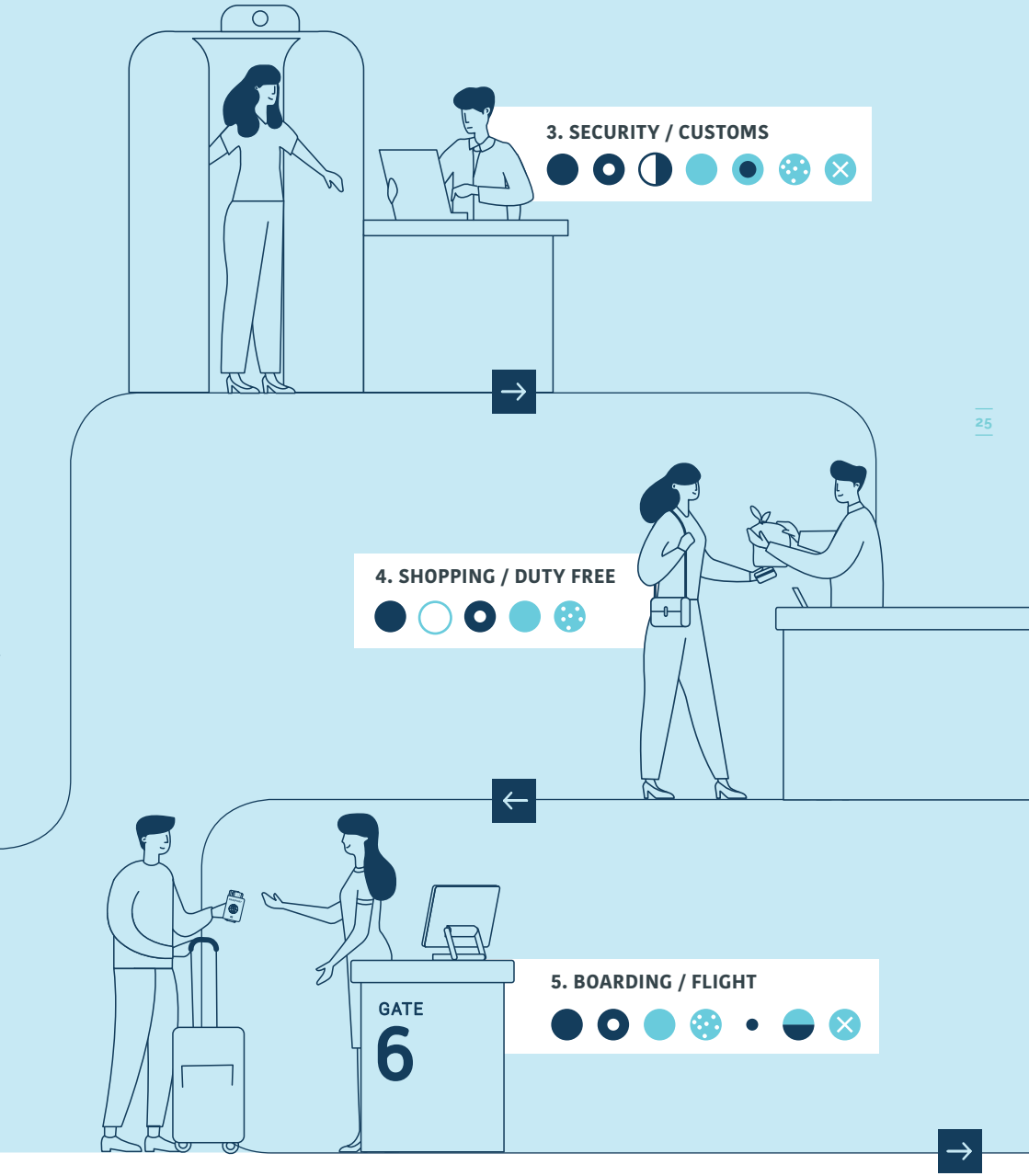
Information screens

Handling luggage

Processing passenger data

Security systems

Passenger devices



Connection with administrative bodies

Connection with airport service providers

Connection with airlines

Runways

Exchanges with European ATC systems

THE 10 MUST-ASK QUESTIONS

**Cybersecurity is complex and may seem difficult to grasp.
Here are ten essential questions that will provide food for thought**

01 **WHO IS MY CISO?**

The Chief Information Security Officer must be a regular participant in the life of the company.

02 **WHEN WAS THE LAST TIME I HEARD ABOUT CYBERSECURITY?**

Being regularly informed is essential to having a clear and optimized approach, and also for developing skills.

03 **WHEN DOES THE AIRPORT TALK ABOUT CYBERSECURITY IN-HOUSE?**

Raising team awareness is an essential stage in dealing with the human risk factor. Communications on best practices to be implemented must be regularly scheduled.

04 **WHAT IS THE THREAT INTENSITY FACED BY MY AIRPORT?**

Airports are attractive targets. What volume and frequency of attack should I expect? Has a major attack already been fended off or thwarted?

05 **WHAT IS MY PERSONAL LEVEL OF RISK?**

Everyone has a potential risk factor, which increases with the level of responsibility. Have I adopted the most appropriate best practices?

06 **WHAT ARE MY MAIN FEARS?**

Focusing on the five most significant risks will help in establishing and pursuing a coherent strategy.

07 **WHO ARE MY BEST POINTS OF CONTACT?**

Do I know who to contact according to the circumstances? Is it possible to contact this person / these people easily? Can they respond quickly enough?

08 **WHEN WAS THE LAST AUDIT?**

Critical vulnerabilities can be detected by carrying out audits and penetration tests. They must be carried out regularly in order to take into account the shifting development of threats.

09 **IS THERE A CRISIS PLAN?**

Best practices reduce risks, but new behaviour is necessary in the event of a crisis. All companies must be trained to react appropriately.

10 **WHAT ARE THE LEGAL RISKS?**

The airport may be held liable in the event of poor protection. Up to what point and how is the airport exposed to such risk?

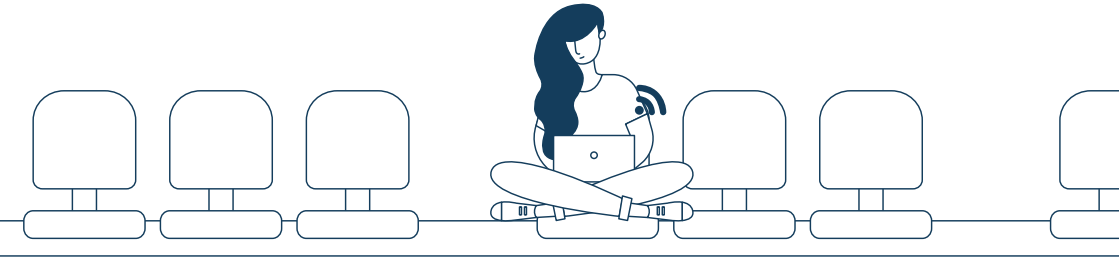
HUMAN RISK FACTORS

All the studies on attacks and cybersecurity agree on one point: although the technical aspect is important, the human aspect is of even greater importance. **The success of any malicious data leakage or attack is mainly due to human negligence or ignorance,** phishing and password theft (by looking at someone entering their password) concerning the individual and not the device.

There are two user habits that must be very closely monitored and which should be subject to in-house policy: the **use of a personal laptop or smartphone** as a work tool (especially if connected to the company's network) and **visiting Internet websites and social networks,** frequent sources of phishing campaigns by email or sms.

INCREASING BOTH SKILLS AND KNOWLEDGE IS ESSENTIAL

There are technical solutions to limit risks: blocking access to certain websites, using mobile fleet management software, establishing an effective firewall, checking rights of access to sensitive documents, etc. However, training everyone to follow a set of best practices and **increasing both skills and knowledge is essential.**



Airport personnel are not the only populations at risk. An airport is, by definition, a **zone of exchange and transit** for passengers and those accompanying them. Indeed this population largely outnumbers those working at the airport and although their interactions with systems and facilities are limited, they are nevertheless a source of risk. The difficulty is that only passive actions are feasible – protection of public WiFi, sensitive connected devices, etc. as **passengers are not obliged to adhere to the best practices imposed on the teams** of airport personnel. They are also customers so it is a question of finding a balance between meeting their demands and protecting the airport organisation.

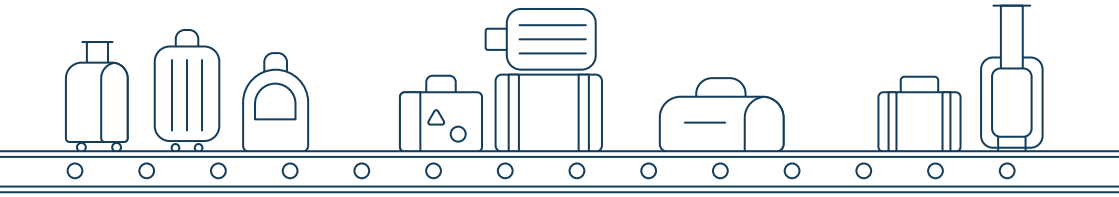
IN 2012, A LORRY DRIVER EQUIPPED WITH AN ILLEGAL GPS JAMMER INTERFERED WITH THE SIGNALS USED BY THE GROUND NAVIGATION SYSTEM AT NEWARK AIRPORT.*

* Source : FCC, FAA

RISKS ASSOCIATED WITH FACILITIES AND INFRASTRUCTURE

Airports have a particular requirement of protection both with regards to their own IT infrastructure – network, computers, servers, etc. – and also the adjacent physical infrastructures, such as the building itself (ventilation, heating, video-surveillance, etc.), luggage sorting facilities, car parks, runway signage, etc. These facilities are increasingly computerized and connected so they are potential vectors of attack, and are even more vulnerable because, up to now, they have benefited from very little protection. Contrary to what one might believe, **any device, even one that is not connected to the network, may be the target of an attack,** for example through a virus infected flash drive. The consequences can be dramatic, ranging from the leakage of sensitive data to a total interruption of the service.

Access to sensitive equipment and facilities should, therefore, be limited and controlled, in both the digital world and the physical one. This involves setting up physical barriers (alarms, cameras, badge access, etc.) and virtual barriers (authorisation, antivirus, intrusion detectors, etc.) These must be **regularly tested and updated.** According to the size of the airport and the loss incurred by service disruption, redundant installations will be necessary for critical facilities, especially for backing up systems and resources.



Finally, business continuity plans should be drawn up for each category of facility or vital resource and be tested as regularly as possible.

Now perceived as an essential **by passengers, public WiFi must be kept separate from the airport's private network** in order to avoid any contamination.

FOLLOWING AN ATTACK ON THE CITY'S IT SYSTEMS, THE AIRPORT OF ATLANTA TOOK THE PRECAUTION OF CUTTING ITS PUBLIC WIFI FOR A PERIOD OF ONE WEEK.*

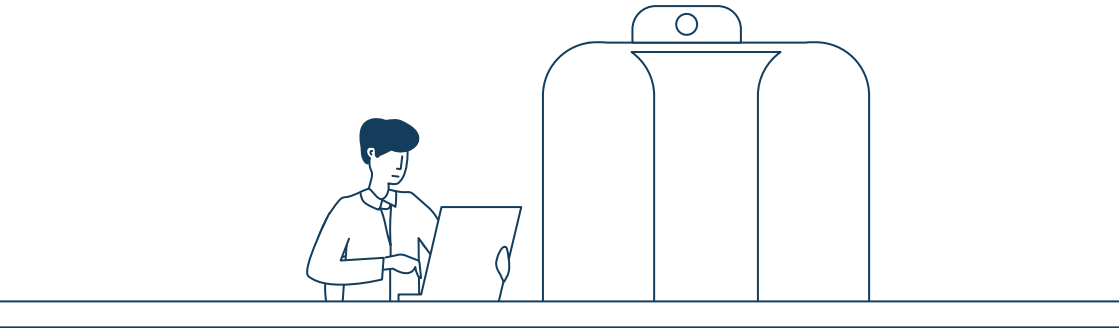
* Source : AFP

RISKS ASSOCIATED WITH PARTNERS

An airport ecosystem is complex and comprises multiple service providers and partners working in various fields: airline companies, dealerships, security services, cleaning companies, etc. So there are many stakeholders who, as part of their relationship with the airport, have direct or indirect access to certain facilities and sensitive data. **Each person must carry out a risk analysis of their scope of activity and act accordingly.**

An essential component is the signature of contracts framing the use of systems and data, and requiring absolute compliance with the best practices laid down by the airport, backed by the setting up of protocols and procedures. Contracts must **also stipulate the liabilities of each party in the event of hacking.** It is, moreover, possible to contractually impose training in cybersecurity best practices, adjusted to suit each level of risk. A consultant with access to the airport's information systems must know its internal practices, whereas a cleaning service provider or security agent can settle for a more general training course. It is necessary to ask for a certificate or quality label providing assurance that the partner has the skills necessary to implement the airport's cybersecurity policy.

ENSURING THAT THE PARTNER HAS THE NECESSARY SKILLS



Particular attentions must be paid to service providers operating in the Cloud. Sometimes dealing with the company's critical systems, they have the same risk profile coupled with the **disadvantage that the protective measures set up are not within the airport's remit.** So having recourse to such services must be formally determined by the different stakeholders and be set up within the scope of a contract.

IN 2015, AN OUTAGE OF THE LOT POLISH AIRLINE'S INFORMATION SYSTEM DISRUPTED TRAFFIC AT CHOPIN AIRPORT IN WARSAW FOR 5 HOURS, GROUNDING SOME 1,400 PASSENGERS.*

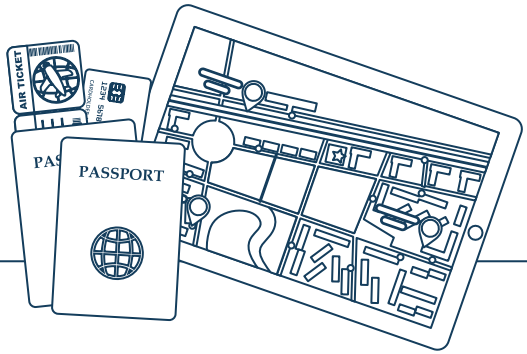
* Source : LCI

RISKS ASSOCIATED WITH DATA

A great deal of sensitive data circulates in an airport: flights schedules, bank transactions, passengers' personal data, etc. A management policy must be set up and implemented by one or several managers in order to limit the risks. Access to the listed and categorized data is consequently restricted and controlled, and undergoes regular updating. **Having predetermined plans of action, to implement in the event of attack or data leakage, is also of utmost importance.**

With the GDPR, processing of personal data is subject to new requirements; **non-compliance can lead to severe financial sanctions** (4% of worldwide sales, or 20 million euros...). Notably, **customers and employees have rights with regard to access, modification, portability and deletion of their data.** Ensuring and overseeing compliance over time is the responsibility of the DPO (Data Protection Officer), playing a new role within the company.

Aside from this appointment, the company's organisation is barely affected by compliance alignment, which above all concerns processes. These must be analysed in order to be developed accordingly, which is sometimes just a simple question of updating contact forms on the website. Occasionally, it is necessary to change the solution and train all the users.



The GDPR has also introduced the sharing of responsibility between the airport, its partners (airline companies, amongst others) and its service providers. Contracts must keep pace with these developments to ensure that such partners and service providers are, themselves, in compliance with the Regulation.

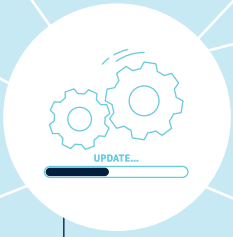
IN 2017, A NON-ENCRYPTED FLASH DRIVE WAS FOUND IN A LONDON STREET. IT CONTAINED CONFIDENTIAL DATA ABOUT HEATHROW AIRPORT SECURITY, AND PARTICULARLY THE ITINERARIES TAKEN BY THE QUEEN AND SEVERAL MINISTERS. MEDIA REPORTED THAT THE AIRPORT OPERATOR WAS FINED BY THE INFORMATION COMMISSIONNER'S OFFICE FOR "SERIOUS DATA PROTECTION FAILINGS". THE AIRPORT TOOK ACTIONS TO STRENGHTEN ITS PROCESSES AND PROCEDURES.*

* Sources : The Mirror / BBC

BEST PRACTICES TO BE ADOPTED

Everyone in the company must adopt best practices to ensure mitigation of the risks faced by the airport, to the point that they become instinctive.

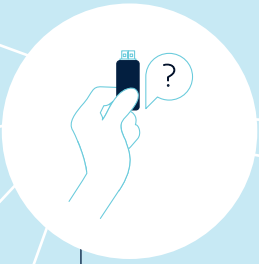
02
Back up files frequently



03
Update staff terminals

01
Clearly define and use password policies: do not use them in public, do not communicate them...

04
Protect connection when using public WiFi, and do not consult confidential documents



06
Do not use external storage media (CD, flash drive, etc.) without knowing their source

07
Do not click on an attachment or link if you don't know the person who sent it

08
Switch off your devices in the evening

05
Avoid transferring professional data to personal accounts

09
In the event of an attack or alert, log out from the network

10
Regularly monitor personal social media accounts to be able to react promptly in the event of sensitive information being posted

BRINGING YOUR ORGANISATION UP TO SPEED

It is necessary to have someone in charge of ensuring the application of a global cybersecurity strategy. This CISO does not have a predetermined position in the company's organisational chart: **the most important consideration is that the CISO optimises his effectiveness.** Given the transversal nature of risks, he should be able to act in all the airport's trades and, if necessary, have intermediaries. To accelerate the decision-making process, his position in the chain of command is close to executive bodies.

Finally, his mandate must be clear and well-defined: legal and operational responsibilities, delegation of power, etc. **A CISO is able to determine strategic, technical and organisational choices within the framework of governance involving business line managers.**

As for the **DPO,** who has specific skills and knowledge, **he should benefit from material and organisational means, resources and position enabling him to perform these missions.**

Best practice consists in separating the duties of the DPO and CISO, the first deals with compliance and the second with cybersecurity. However, depending on the size of the airport, both tasks can be carried out by the same person.

WHAT BUDGET TO EARMARK FOR CYBERSECURITY?

According to the French National Cybersecurity Agency (ANSSI), between 3% and 10% of the IT budget should be earmarked for cybersecurity. The proportion varies according to the size of the airport; an average-size airport will not have the same needs as an international airport.

This budget is divided into three main items:

- cyber defence (protection, detection, reaction);
- communication (training and raising awareness);
- governance procedures.

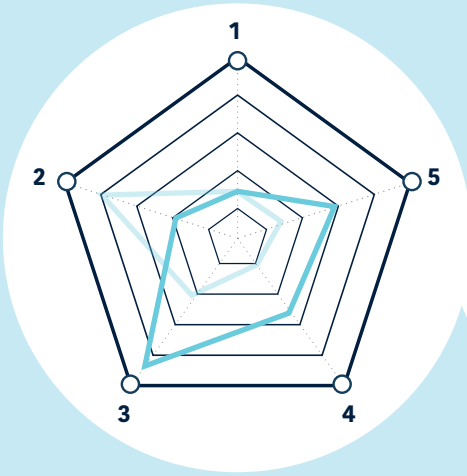
Apart from these technical and organisational aspects, other measures must be included in the company's other budgets: maintaining all technical means secure, upgrading available technical means and adjusting procedures as appropriate. In addition, **each project must include cybersecurity actions, which requires an increase in budget of 2 to 5%.**

BETWEEN 3% AND 10% OF THE IT BUDGET SHOULD BE EARMARKED FOR CYBERSECURITY

When reflecting on this matter, do not forget that **cybersecurity is a profitable investment,** compared with the potential losses that might arise from a cyberattack. Furthermore, **it contributes to the creation of company value** by instilling trust in customers and partners.

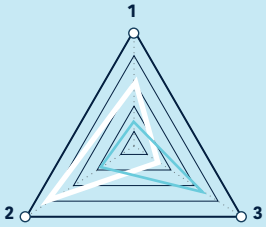
EXAMPLES OF INDICATORS

Building dashboards with key indicators is essential.
It is just as vital to monitor their development over time.



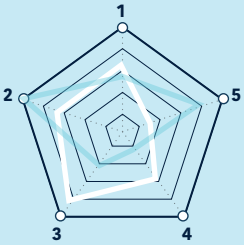
1 • Strategy
2 • Compliance
3 • Finance
4 • Operational
5 • HR

Example 1 HR



1 • Actions carried out
2 • Training courses
3 • Skills

Example 2 Operational



1 • Accidents
2 • Audits
3 • Vulnerability Tests
4 • Updates
5 • Shadow IT

PROTECT OVER THE LONG TERM

Cybersecurity is a never-ending task. It would be a mistake to think that the file can be closed once you have carried out all the necessary transformations. By its very nature, cybersecurity is a **continual process of improvement** and so it is essential to be ready to step up to the challenge and adapt to new threats, raise awareness among staff with regard to new risks and take into account the additional workload that cybersecurity represents. All users are concerned by this issue and must engage in dealing with it.

It is, therefore, a question that must be regularly raised at all levels within the airport, from the board of directors to the employees. Within the framework of a defined global strategy, cybersecurity is subject to **regular reviews** backed by relevant indicators. **The construction of clear and understandable dashboards,** taking into account all these factors, is an essential task that must not be overlooked.

CYBERSECURITY IS A DAILY FIGHT: DON'T DROP YOUR GUARD.

Likewise, the **proficiency of everyone in the company must be tested and regularly updated.** This also applies to best practices with an arsenal of ad hoc training courses, communication tools, etc.

PART 3

PRACTICAL INFORMATION

BIBLIOGRAPHY

SECURING SMART AIRPORTS
www.enisa.europa.eu
ENISA, 2016

ADDRESSING AIRPORT CYBER SECURITY
www.sesarju.eu
SESAR joint undertaking, 2016

GUIDE TO INDUSTRIAL CONTROL SYSTEMS SECURITY
nvlpubs.nist.gov
NIST Special Publication, 2013

GUIDEBOOK ON BEST PRACTICES FOR AIRPORT CYBER-SECURITY
www.trb.org
ACRP Report 140, 2015

ACI WORLD - AIRPORT IT STANDING COMMITTEE (AITSC) REPORTS AND TOOLS (INCLUDING A BENCHMARKING TOOL)
www.aci.aero

AIRPORT INFORMATION TECHNOLOGY & SYSTEMS (IT&S) BEST PRACTICE GUIDELINES FOR THE AIRPORT INDUSTRY
www.acconline.org
Airport Consultants Council, 2012

ANSSI BEST PRACTICES (FRANCE)
www.ssi.gouv.fr

PREPARING FOR THE GDPR
www.eugdpr.org

STANDARDS
www.iso.org

ISO 27002 STANDARDS
www.iso.org

CYBER CRIMINALITY, THE NEW WEAPONS FOR POWER
Solange Ghernaouti
Editions PPUR, 2017

THE ESSENCE OF DIGITAL SECURITY FOR COMPANY DIRECTORS
Nostromo
Editions Eyrolles, 2017

CYBERSECURITY BEYOND TECHNOLOGY
Philippe Trouchaud
Editions Odile Jacob, 2016

WHAT DO I KNOW ABOUT CYBERSECURITY?
Nicolas Arpagian
Editions PUF, 2015

GLOSSARY

ADVANCED PERSISTENT THREAT (APT)
A stealthy attack in which a non-authorised person gains access to the network and remains undetected for an extended period of time. The aim is to steal data rather than damage the network.

AUTHENTICATION / IDENTIFICATION
Identifying yourself means communicating your identity; authentication means providing proof of your identity.

BACKDOOR
Hidden access, either software or hardware, that enables an attacker to secretly connect to a machine.

CRYPTOLOCKER
A particular type of ransomware, mainly disseminated through infected emails, which encrypts the user's data.

DEFACEMENT
Result of malicious activity that modifies the appearance or contents of a Web server.

DENIAL OF SERVICE (DOS)
Attack that results in preventing or substantially limiting the capacity of a system to provide an expected service.

ENCRYPTION
Cryptographic transformation of data producing a cryptogram, i.e.: a set of encrypted data.

FIREWALL
A firewall is a tool that provides protection for a computer connected to a network or Internet. It defends against external attacks (filters incoming traffic) and often illegitimate connections to the exterior (filters outgoing traffic) triggered by programs or people.

FLAW
Vulnerability in an information system enabling an attacker to damage its normal function, confidentiality or integrity of the data it contains.

HACKTIVIST
Hacking a website or network for a political motive (e.g. convey a message, cause disruption etc.)

HOAX
False information, often transmitted by electronic messaging or in a forum, and inciting recipients to carry out transactions or take initiatives, that often cause damage.

KEYLOGGER
Software or material used by a malicious actor to record what a person is typing on the keyboard.

MAIL HARVESTING
Action that consists in surfing a large number of public resources (Internet pages, discussion groups, etc.) in order to collect email addresses for malicious intent.

MALICIOUS SOFTWARE, MALWARE
Any program developed in the aim of doing damage: virus, Trojan horse, etc.

MALVERTISING (MALICIOUS ADVERTISING)
Use of online advertisements to disseminate malicious software.

PENETRATION TEST (PEN TEST)
A controlled action that attempts to evaluate one or several vulnerabilities through a simulated attack on an information system.

PHISHING
Theft of identities or confidential information (access codes, bank details, etc.) by subterfuge: a fake authentication system is simulated by an attacker who then tries to convince the targeted victim to use it and communicate confidential information in the belief that it is a legitimate system.

PRIVILEGE ESCALATION
Unlawfully obtaining IT rights. A person wishing to do harm seeks to gain elevated access when entering an information system by usurping the identity of a legitimate user.

RANSOMWARE
The term “ransomware” is a contraction of the words “ransom” and “software”. It is a type of malicious program, the aim of which is to force the victim to pay a ransom.

SECURITY INCIDENTS
An event that harms the availability, confidentiality or integrity of an IT resource. Examples: illegal use of a password, theft of IT facilities, intrusion in a file or application, etc.

SPYWARE
Software that aims to collect information about the environment in which it is installed and the habits of the system’s users, and then transfer this information to third parties, without the knowledge of the data owner and legitimate user.

TROJAN HORSE
Program giving a misleading impression of having a useful function, but additionally having a hidden function that is potentially malicious.

VIRUS
A virus is a malicious program or part of a program, the aim of which is to survive in an IT system (computer, server, mobile device, etc.) and very often to damage or infect resources (data, memory, network). The mode of survival can take several different forms: replication, implantation within legitimate programs, persistence in memory, etc. A virus uses all available means in order to spread: messaging, file sharing, backdoor, fake Internet page, flash drives, etc.

VULNERABILITY
Technical weakness of an information system present in the specifications, design, creation, installation or configuration of a systems, or in the way it is used.

WATERING HOLE
Attack intended to infect the computers of personnel working in a business sector or a targeted organisation, by booby-trapping a legitimate Internet website in order to infect visitors’ devices.

ADDRESSES

AFCDP
Association française des correspondants à la protection des données personnelles
(French association of data protection officers)
www.afcdp.net

AFPI
Association française des prestataires de l'Internet
(French association of internet service providers)
www.afpi-france.com

ANSSI
Agence nationale de la sécurité des systèmes d'information
(French National Cybersecurity Agency)
www.ssi.gouv.fr

BEFTI
Brigade d'enquêtes sur les fraudes aux technologies de l'information
(Brigade for the investigation of information technology fraud)
01 55 75 26 19

CESIN
Club des experts de la sécurité de l'information et du numérique
(Club of information and digital security experts)
www.cesin.fr

CESYF
Centre expert contre la cybercriminalité français
(French centre of experts working to combat cybercrime)
www.cecyf.fr

CLUSIF
Club de la sécurité de l'information français
(French information security club)
www.clusif.fr

CNIL
Commission nationale de l'informatique et des libertés
(French national commission for data protection)
www.cnil.fr

CYBERLEX
Association du droit et des nouvelles technologies
(Law and emerging technologies association)
www.cyberlex.org

IHEDN
Institut des hautes études de défense nationale
(Institute of higher national defence studies)
www.ihedn.fr

INHESJ
Institut national des hautes études de la sécurité et de la justice
(National institute of higher security and justice studies)
www.inhesj.fr

OCLCTIC
Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication
(Central office for action to combat crime connected with information technology and communication)
01 49 27 49 27

CONTACTS

UAF&FA
Union des Aéroports Français & Francophones Associés
The French and French-speaking airports association
www.aeroport.fr

ACI
Conseil International des Aéroports
Airports Council International
www.aci.aero

EUROCONTROL
www.eurocontrol.int

EASA
Agence européenne de la sécurité aérienne
European Aviation Safety Agency
www.easa.europa.eu

REPRÉSENTATION PERMANENTE DE LA FRANCE À L'OACI
Permanent representation in France of the International Civil Aviation Organization
oaci.delegfrance.org

EUROPEAN AND NORTH ATLANTIC (EUR/NAT) OFFICE OF THE INTERNATIONAL CIVIL AVIATION ORGANIZATION (ICAO)
www.icao.int/EURNAT/Pages/welcome.aspx

In this day and age, cybersecurity is a topic of paramount importance, and one that changes rapidly: new regulations, threats, mitigation measures....
What is the scale of risk faced by airports? How can airports be protected? What are the impacts on airport organisation? What must be known in order to begin or improve the process? This practical guide provides food for thought.

UAF & FA
UNION DES AÉROPORTS FRANÇAIS & FRANCOPHONES ASSOCIÉS