Implementing Cyber-Security Measures in Airports to Improve Cyber-Resilience

Georgia Lykou, Argiro Anagnostopoulou, Dimitris Gritzalis
Information Security & Critical Infrastructure Protection (INFOSEC) Laboratory
Dept. of Informatics, Athens University of Economics & Business, Greece
{lykoug, anagnostopouloua, dgrit}@aueb.gr

***Abstract*- Airports are at the forefront of technological innovation, mainly due to the fact that the number of air travel passengers is exponentially increasing every year. As a result, airports enhance infrastructure's intelligence and evolve as smart facilities to support growth, by offering a pleasurable travel experience, which plays a vital role in increasing revenue of aviation sector. New challenges are coming up, which aviation has to deal and adapt, such as the integration of Industrial IoT in airport facilities and the increased use of Bring Your Own Device from travelers and employees. Cybersecurity is becoming a key enabler for safety, which is paramount in the aviation context. Smart airports strive to provide optimal services in a reliable and sustainable manner, by working around the domains of growth, efficiency, safety and security. This paper researches the implementation rate of cybersecurity measures and best practices to improve airports cyber resilience. With the aim to enhance operational practices and develop robust cybersecurity governance in smart airports, we analyze security gaps in different areas including technical, organizational practices and policies.**

***Index Terms* - Smart Airports, Cybersecurity Best Practices, Industrial IoT Governance, Cybersecurity Management, Critical Infrastructure Protection.**

1. INTRODUCTION

Airport operations and business models have evolved dramatically over the last decades to support the explosive growth of the global aviation industry [1]. Regulatory reform in the new air travelling era produced dramatic traffic growth, diversity and choice for airline passengers. As airlines refine their operating models to align growth to efficiency, airports evolve in parallel to create massive networks of hubs and intelligent systems, which together create an efficient air transportation ecosystem [2].

Airports are considered a gateway to the world for travelers and business, thus they are of great importance for country development and economic growth [3]. In USA, aviation and airports, as transportation subsector, constitute a critical infrastructure and key resource sector, according to the U.S Homeland Security Presidential Directive [4]. The same applies in Europe, where critical infrastructures and essential services in air transport facilities should be adequately protected according to NIS & EPCIP directives and EC/216/2008 regulation [5-6].

Securing Smart airports and staying ahead of evolving cyber threats is a shared responsibility, involving airlines, airports, vendors and regulators [7]. Identification of challenges posed by cyber threats, risk assessment approaches and guidelines to enhance cyber security, either in terms of high level governance strategies and specific technological support are priorities currently researched in aviation industry.

This work aims to identify cybersecurity policies in airports operating intelligent services, while taking stock of measures and good practices already implemented. Our purpose is to develop robust cyber security framework in commercial airports, by analyzing security gaps in different areas including technical, organizational practices and policies. The rest of this paper is structured as follows: airports classification based on technological evolution is presented in section 2. The methodology used for this research follows in section 3, while in section 4 online survey results are analyzed, along with implementation security practices presented in section 5. The significance of our findings is discussed in section 6, while section 7 concludes our research work.

2. AIRPORT INTELLIGENCE CLASSIFICATION

Increasing their infrastructure complexity, airports have gained more stakeholders nowadays. They have honed their capabilities in interoperability by using Internet of Things (IoT) technology and intelligent applications to achieve on effectiveness. According to Pethuru [1], there is an evolution pace in today's airports, which can be classified into three broad categories:

In the Airport phase 1.0 (Basic), airports focus on capabilities necessary for safe and efficient management of landings, departures, and other aircraft operations. They offer basic passenger services, including check-in, boarding, security, baggage pick-up, and moderate retail, food, and beverage services.

In the Airport phase 2.0 (Agile), airports adapt to this changing digital environment. Technology enabled collaboration is highly evolved throughout these airports and is implemented across business units. Airport-wide, converged network architecture offers shared services on a common platform.

In the Airport phase 3.0 (Smart), airports fully exploit the power of emerging and maturing technologies of IoT, with advanced and pervasively deployed sense-analyze-respond capabilities. The digital grid is the airport's nervous system, touching and managing every point of interaction. By enabling the exchange of real-time information, profound collaboration, and airport-wide process integration, smart airports significantly improve operational efficiencies, passenger services, and advanced security capabilities.

According to ENISA, smart airports are those who make use of networked, data driven response capabilities that, on the one hand, provide travelers with a better travel experience and, on the other hand, aim to guarantee higher levels of security for the safety of passengers, operators and general public [7]. Since, safety and security are the most significant domains in aviation context, a safe environment must be ensured by proactively handling difficult cyber challenges, while minimizing operations disruption.

Cyber security can be defined as the collection of tools, policies, security safeguards, guidelines, risk management approaches, training, best practices, assurance and technologies used to protect the cyber environment and organizations' assets. Although many airports have robust systems in place to address common hacking threats, they haven't always taken a holistic approach to the IT cyber environment or considered the broader threat to the aviation system [8]. In this direction, International Civil Aviation with ICAO/A39 calls on states and industry stakeholders to encourage coordination with regard to aviation cybersecurity strategies, policies and sharing of information to identify critical vulnerabilities that need to be addressed, by developing systematic information sharing on cyber threats, incidents and mitigation efforts [9].

Particular to airport cyber security, risks constantly change as new threats and vulnerabilities surface along with ever-changing technology implementations. A taxonomy of threats to the cyber security of smart airports, including mapping to smart airport assets has been developed by ENISA and makes evident that cybersecurity has a major stake in providing safety. The challenge is to address security issues not only to enhance security but also to ensure safety [7].

3. RESEARCH METHODOLOGY

This work has been developed using a combination of literature research and information received from an online survey about airport cybersecurity. The survey was addressed to European and American busiest airports with the purpose to understand the opinion of airport IT personnel about the introduction of the IoT to their airports and the cybersecurity measures applied. All survey responses received were promised to be treated with confidentiality and data from this research would be reported only in the aggregate.

Our goal was to define the implementation rate of cybersecurity best practices in combination with IoT application status, through IT personnel opinions. Since there was a great diversity of technological evolution in airports examined, we have made an aggregated analysis of responses, combined with airport classification presented in Section 2.

4. SURVEY RESULTS

The questionnaire was addressed to more than 200 airports in Europe and USA, but only one third of them had responded to the survey. Among them, we distinguished 34 fully completed questionnaires with sensible answers and we elaborated their results. Answers received from European airports reached 66%, while 34% came from USA. The airports have been further classified to Basic/Agile/Smart categories, according to their own statement about being or planning to be smart, in combination with the number of IoT applications, they indicated to use in their facilities. This classification was chosen, in order to better evaluate the cyber-security preparedness level of airports, based on ICT complexity and technological progress. As a result, 16% of airports have been classified in Basic category, 55% were categorized as Agile and the rest 27% of airports were ranked as Smart airports.

Although 59% of responders have stated to have effective cybersecurity policies for IT assets, when they were asked to rank the risks from IoT devices, the majority (76%) pinpointed the lack of security awareness as the greatest risk, followed by internet connectivity risk (29%), which reveals a controversy in security confidence of responders.

Airports have defined which smart applications are using in their facilities that underpin key airport activities, as listed in Fig. 1. As we can see, the most popular smart applications are passenger check in & boarding services (41%), common use passenger processing systems (41%), while the least used are SCADA applications (6%) and connections with other transport systems (15%).

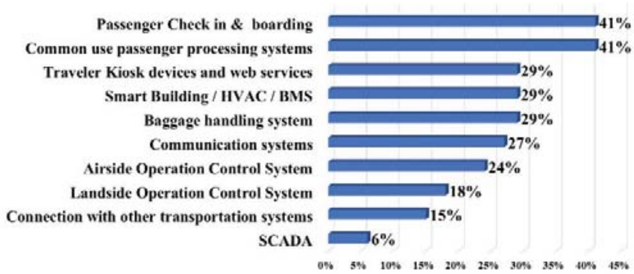

Fig.1. IoT Applications in Airports

Especially in smart airports, IoT applications like baggage handling, passenger check in, landside operation controls, common use passenger services and traveler web services are found to be used in frequencies over 70%. Building Management Systems (BMS) and HVAC equipment controls are also widely used in smart airports (60%). SCADA systems are in their infancy stage overall in airports. Only smart airports have stated to use SCADA with a 20% implementation rate.

Since industrial IoT are in their emergence, a great expand is expected to transform mainstream busiest airports to smart airports. Research revealed that this early adoption increases smart airport's interoperability, along with vulnerability exposure to cyber threats [2], [7].

5. SECURITY PRACTICES FOR SMART AIRPORTS

Securing Smart airports and staying ahead of evolving cyber threats involves proper management from all stakeholders. Security good practices and tools have been developed and published in literature [3], [7], [10-15]. The identified practices for smart airports have been categorized into three main groups: i) Technical; ii) Organizational and iii) Policies and Standards, as presented in Fig. 2.

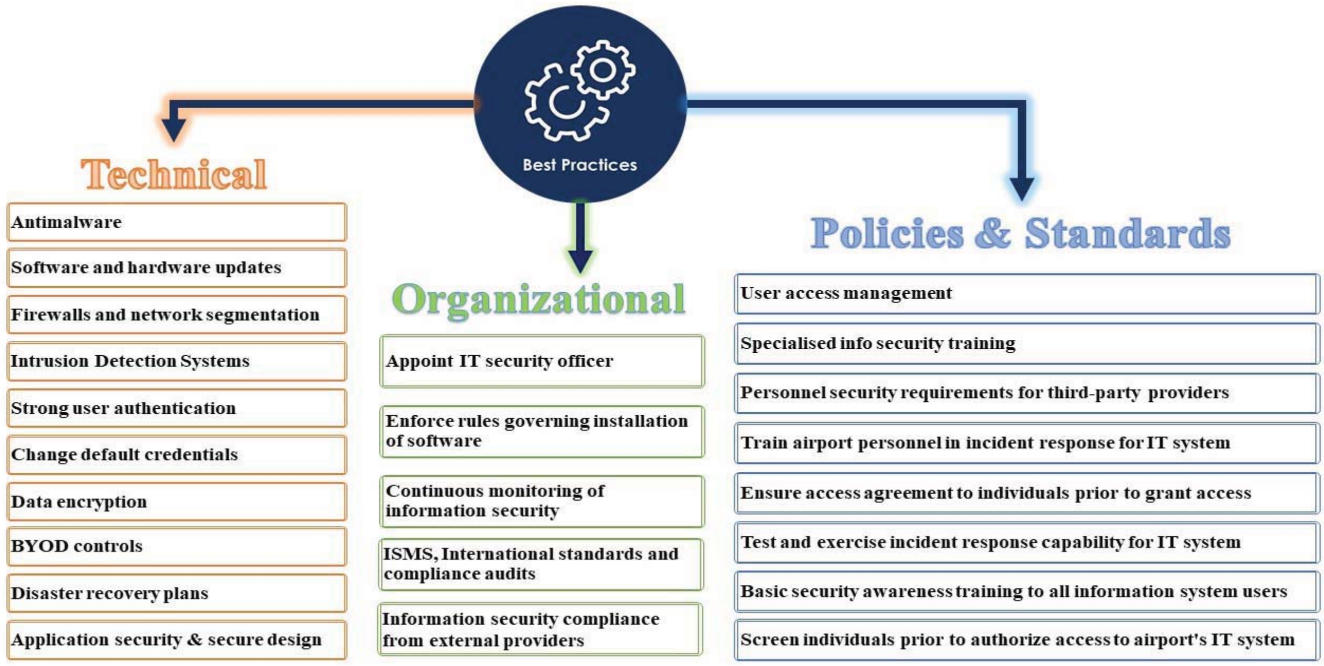

Fig. 2. Cyber Security Good Practices Classification

5.1. Technical Good Practices

There are various good practices published for all aspects of airport-based technical practices. Below we provide an overview of ten good practices included in our survey, followed by airport responses analysis.

Antimalware: All computers should run anti-malware software to detect and remove or quarantine malicious software. Smart airports have responded to apply at 60% rate antimalware practices to IT equipment, agile airports are partly implementing with 50% rate, and basic airports poorly implemented antimalware protection reaching only 33%.

Software and hardware updates: Should be regularly performed. Applying security patches prevents cyber criminals exploiting unpatched software and reduces the exposure to known vulnerabilities. This was implemented at 80% rate from smart and agile airports, while only at 33% rate from basic airports.

Firewalls and network segmentation: The border of the airport network infrastructure should be protected by perimeter firewalls to block untrusted connections between networks. A defense in depth approach should be taken to improve network security. Both smart and agile airports fully comply with these practices (100%), while basic airports perform above average with a 67% implementation rate.

Intrusion Detection Systems (IDS): Refers to monitoring of both software and hardware devices over the network. It can be categorized as (i) network-based IDS, focused on the analysis of network traffic and (ii) host-based IDS, able to analyze activities on the host and raise alerts, in case of events like unauthorized access to applications, escalation of privileges, modification of file systems, etc. Smart and agile airports reported to implement IDS at 60% rate, which reveals a security gap, especially for smart airports with many integrated applications and communication ports. Basic airports were found not to implement at all this practice, which creates a serious vulnerability and security risk.

Strong user authentication: Should protect IT devices, while sensitive or remote services should require access only via multifactor authentication and/or biometric identifiers. Smart airports responded to protect IT services using strong authentication (80%), agile airports comply less (60%), while basic airports not at all.

Change default credentials of devices: Devices, connected to the airport network should be properly configured and have default password changed. In addition, when not required, remote access should be disabled to prevent cybercriminal remote-connection attacks. Here the compliance was poor for all airports categories (smart 40%, agile 50%, basic 33%) which revealed a security gap and a serious vulnerability.

Data encryption: Used to protect sensitive information exchanged in the network from eavesdroppers and to protect data collection and storage. Smart airports satisfactory use encryption methods at 80%, agile airports have lower implementation rate reaching 50%, while basic airports do not use encryption methods, according to IT personnel responses.

Bring your own device (BYOD) controls: Airports should typically prevent employees from connecting their own personal devices to airport systems. Otherwise, effective technical controls should be applied to protect the airport and network infrastructure from compromised devices. All airport categories seem to poorly apply controls for such devices (smart 40%, agile 33%, basic 0%), which reveals the need for security reinforcement with suitable measures to increase cybersecurity protection.

Disaster recovery plans for IT assets: Technical procedures should be in place to restore operation of critical IT assets to an adequate level of service, in case of emergency. Both technical and organizational aspects must be included in disaster recovery plans. People involved must have a clear view of their roles, the sequence of actions to be performed, the actors involved and so on. All smart airports responded positively for this practice with 100% rate, agile airports implementation reached 60%, while for basic airports only one third stated to apply such procedures for IT assets.

***Application security and secure design*:** Secure design should be part of System/Services/Technology Acquisition. It should be combined with airport assets under provisioning risk assessment, privacy by design principle and security criteria requirements. Smart airport responded at 80% to apply secure design procedures, while agile and basic airports had only at one third implemented this practice.

TABLE I. TECHNICAL GOOD PRACTICES

Technical Good Practices	BASIC	AGILE	SMART	ALL
Antimalware	33%	50%	60%	50%
Software and hardware updates	33%	80%	80%	72%
Firewalls & network segmentation	67%	100%	100%	94%
Intrusion Detection Systems	0%	60%	60%	50%
Strong user authentication	0%	80%	60%	61%
Change default credentials	33%	50%	40%	44%
Data encryption	0%	50%	80%	50%
BYOD Controls	0%	30%	40%	28%
Disaster recovery plans	33%	60%	100%	67%
Appl. security & secure design	33%	30%	80%	44%
Average implementation rate	**23%**	**59%**	**70%**	**56%**

Table I presents the technical good practices implemented in all airports categories, based on survey answers and airport classification. As we can notice, the most implemented technical based practices for all airports are: i) Firewalls and network segmentation (94%); ii) Software and hardware updates (72%); and iii) Disaster recovery plans (67%). On the contrary, the least implemented technical based practices are: i) BYOD Controls (28%); ii) Change default credentials (44%); and iii) Application security and secure design (44%).

Smart airports have the greatest implementation rate of technical practices, reaching 70% on average. This was an expected result, since advanced complexity of smart applications, requires advanced cybersecurity defense. However, we have found that some practices were poorly implemented by smart airports, such as changing default credentials and BYOD controls, which reveals a security gap and possible areas for cybersecurity amelioration.

Agile airports have an overall lower implementation rate of technical practices, reaching on average 59%. They are all implementing firewalls & network segmentation, while the majority uses strong authentication and software/hardware updates. However, they lack of applying technical practices, like BYOD Controls and secure application design.

Basic airports need to start implementing practices like: Data encryption; Strong user authentication; BYOD controls and IDS, since they have responded not to apply at all. Besides, they need to enforce all the other technical practices. The most implemented measures are firewalls and network segmentation at 67% rate, while the average implementation on technical practices is only 23%.

Research also revealed that airports, who are using IoT and SCADA applications in their facilities, have more technical practices implemented than the other airports. This indicates a higher concern about cybersecurity and effective performance towards cyber resilience achievement.

5.2. Organizational Good Practices

A variety of airport-based organizational practices about people and processes exists in literature [2],[7]. Below we provide an overview of each good practice and afterwards we analyze airport responses about their implementation.

***User access control and management**:* Logical and physical access control to airport IT systems should be established along with identity access management system. All airport categories responded to apply such procedures (90-100%), which allies with safety culture already developed, regulated and implemented in airport facilities.

Screen individuals prior to authorizing access to the airport's information system: Requiring airport employees to undergo biometric identification prior to being granted access can be beneficial for mitigating the risk of identity fraud. Smart airports apply this process at 60% rate, agile at 50%, while basic airports not at all, according to their replies. Privacy and personal data protection restrictions and regulations are possible obstacles for biometric applications.

Ensure individuals requiring access to airport IT systems sign appropriate access agreements: Prior to being given access to airport IT systems, individuals should sign appropriate access agreements, including non-disclosure & acceptable use agreements, rules of behavior and conflict of interest agreements. All airport categories responded to poorly implement this practice with 20-40% application rate.

Establish personnel security requirements for third-party providers, including security roles and responsibilities. 3rd party compliance with such requirements should be also monitored. Smart airports apply such security requirements at 60% rate, while only one third from agile and basic airports comply with such security requirements.

Provide basic security awareness training to all information system users based on the specific requirements of the airport and the IT systems. The majority (60%) of smart airports provides such training to system users, responses from agile airports are at 50% and basic airports need to do more on this area (33%), in order to improve cyber resilience. Security awareness was cross checked with other questions within the survey, where responders claimed that the lack of security awareness was a major risk for IoT devices in airports facilities.

Provide specialized information security training with role-based and security-related training, before authorizing access to IT system. The request for specialized security training is a common need for all airports based on survey responses with low implementation rate (33-40%). IT personnel responses revealed the need for more specialized security training to confront the increasing complexity of cybersecurity threats.

Train airport personnel in their incident response roles with respect to the information system: Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources to handle the situation in a way that limits damage and reduces recovery time and costs. The same response attitude from all airport categories with low implementation rate (33-40%) was also found here, which urges for continuous training policies implementation.

Test and regularly exercise the airport's incident response capability system to determine incident response effectiveness and avoid a low level of incident response capability. Airports responded to have a medium implementation of this procedure with smart airports at 60%, agile at 50% rate and basic airports only at 33% compliance.

TABLE II. ORGANIZATIONAL GOOD PRACTICES

Good practices about people, organization and processes	BASIC	AGILE	SMART	ALL
User access management	90%	90%	100%	95%
Screen individuals prior to authorize access to airport's IT system	0%	50%	60%	44%
Ensure access agreement to individuals prior to grant access	33%	20%	40%	28%
Personnel security requirements for third-party providers	33%	30%	60%	39%
Basic security awareness training to all information system users	33%	50%	80%	56%
Specialised info security training	33%	30%	40%	33%
Train airport personnel in incident response for IT system	33%	30%	40%	33%
Test and exercise incident response capability for IT system	33%	50%	60%	50%
Average implementation	**36%**	**44%**	**60%**	**47%**

Table II summarizes employees' responses about airport organizational practices applied to all airports categories. The most implemented security process is user access, reaching 95%, while basic security awareness training to all information system users follows with 56% implementation. The least implemented practices are access agreement for third party stakeholders (28%) specialized security training and incident response for airport's personnel (33%).

Smart airports have a good implementation rate of organizational practices reaching 60%, agile airports have on average low implementation rate reaching 44% and basic airports implement them with the disappointing performance of 36%. Moreover, basic airports seem to ignore basic policies and keep low performance to the majority of organizational practices. This can seriously impact their cyber resilience capability, in case of a cybersecurity incident in critical IT processes and services.

5.3. Policies and Standards

A variety of airport security policies and standards exists in literature [2],[7]. Below we provide an overview of each good practice, included in our survey and then we analyze airport responses about their implementation.

Appoint an information security officer with the mission and resources to develop, implement and maintain an airport-wide information security program. Smart airports have all (100%) appointed an IT security officer. This is obvious a mandatory policy, in order to successfully protect intelligent applications including SCADA and IoT and meet security requirements. Agile and basic airports have a lower performance at 50% and 33% implementation rate for this essential policy, which reveals a serious security inability.

Enforce explicit rules governing the installation of software, in accordance with contract agreements and copyright laws. Specific rules should be established for the types of software that are permitted and which are prohibited. While smart airports have an acceptable implementation rate of 60%, agile (30%) and basic airports (0%) poorly apply such rules, which increases cyber risks and vulnerabilities.

Continuous monitoring of information security should be established and implemented across the airport. The majority of smart airports implements this practice (80%), while agile and basic airports are performing at 50% and 33% rate accordingly. Monitoring strategy and continuous reporting on the security state of the information system should be included in all airports security practices.

Information security management system (ISMS), implement international standards and demonstrate compliance: Organizations following international standards on ISMS should rely on an information security framework, as well as external audits, for measuring progress, identifying gaps and demonstrating compliance. Smart airports are following such practices with 60% rate, agile airports follow with 40% and basic with 33%.

Information Security compliance from providers of external information services should be also certified against relevant standards. An appropriate chain of trust should be established with external service providers when dealing with information security. Smart airports responded compliance at 80% rate, while agile and basic airports reached accordingly 50% and 33% compliance rate.

TABLE III. POLICIES AND STANDARDS

Good Practices for Policies and standards	BASIC	AGILE	SMART	ALL
Appoint IT security officer	33%	50%	100%	56%
Enforce rules governing installation of software	0%	30%	60%	33%
Continuous monitoring of information security	33%	50%	80%	56%
ISMS, International standards and compliance audits	33%	40%	60%	44%
Information security compliance from external providers	33%	50%	80%	56%
Average implementation	**26%**	**44%**	**76%**	**50%**

Table III summarizes IT personnel responses about airport policies and standards applied, according to airport classification and overall. The most implemented security policies are the appointment of IT security officer, continuous monitoring of security, and information security compliance from providers of external IT services. Unexpectedly, the least implemented policy is to enforce rules governing installation of software. This is essential to enhance cybersecurity efficiency, in view of the increase of personal devices interacting with airport's IT systems, combined with the lack of BYOD security controls.

6. DISCUSSION

This survey was developed in order to extract information from airport security professionals about their cyber-security efforts and risk management activities. The decline of participants to fully complete the survey and provide information about their cybersecurity implemented practices was a survey limitation. Indeed, although 280 survey visits have been recorded to the online survey-tool, only 34 questionnaires were taken into consideration in our analysis, due to specific filters applied, relevant to participants' position, along with completeness and robustness of answers received.

Moreover, integrity of responses was partially verified by online search for each airport's technological situation. In our view, this response avoidance was attributed mainly to confidentiality precautions from participants and lack of motivation to support this research work.

Although sample size may be considered as small, it was representative from both Europe and US busiest airports, with a good technological variety of airports between basic, agile and smart categories, so results retain their statistical significance.

7. CONCLUSIONS

Commercial airports are required to develop their own posture to cyber security, nowadays. They are responsible for interpreting existing guidelines & standards and adapting them to suit airport's technological evolution. There is a large variation in how airports design, implement and protect network infrastructure and design cybersecurity solutions. Due to the fact that each airport has a variety of ICT applications being operated within the airport perimeter, the resulting cyber security landscape has a large and complex attack surface.

Our survey revealed the disparity amongst airports in the methods and degree to which cyber security is addressed. While smart airports are having a more mature cyber security posture, basic airports seem to have limited resources dedicated to cyber defense and resilience. Technical based cybersecurity practices have a better implementation rate for all airport categories, while organizational practices, policies and standards keep lower levels of implementation, including low levels of cyber security awareness and training prioritization.

Although smart airports perform the majority of good practices examined in our survey, security gaps have been revealed with poor implementation of IDS, BYOD controls, and changing default credentials. Besides, the rapid advance of IoT technology, along with the slower pace of the legislative processes, may lead to serious legal gaps in digital environment of smart airports. These gaps might pose challenges to airports addressing security and safety.

In addition, there is a need for the identification and development of airport trust framework, helping operators navigate their trust relationships and indicate how smart devices and operators exchange data and operate together. Another important finding of our research was the growing need to educate IT experts and provide specialized training in cybersecurity areas, in order to increase cybersecurity preparedness. Moreover, promoting security awareness of passengers and airports' personnel on the risks posed by new IoT technologies is essential.

Securing Smart airports and staying ahead of evolving cyber threats is a shared responsibility, involving airlines, airports, vendors and regulators. Therefore, a collaborative cyber-resilience model which defines the appropriate cyber security approach for airports is quite important nowadays. Airport operators should prioritize cyber security to ensure safety of operations, passengers and public in general. Cyber threats and risks will continue to grow driven by technological developments, while the relationship between safety and security will become more and more interwoven.

REFERENCES

[1] R.Pethuru, A.Raman, "The Internet of Things: Enabling Technologies, Platforms & Use Cases", CRC Press, 2017.

[2] K. Gopalakrishnan et al. "Cyber security for airports", International Journal for Traffic and Transport Engineering, vol.3, pp. 365-376, August 2013.

[3] J. Urban, "Not Your Granddaddy's Aviation Industry: The Need to Implement Cybersecurity Standards and Best Practices within the International Aviation Industry", Alb. Low Journal of Science & Technology, p. 62, 2017.

[4] Dept. of Homeland Security, "Critical Infrastructure Security and Resilience", PPD-21, 2013.

[5] European Commission, NIS Directive (EU 2016/1148), 2016.

[6] European Commission, The European Program for European Critical Infrastructure Protection (EPCIP), SWD 318, 2013.

[7] ENISA, "Securing Smart Airports", December 2016.

[8] IATA, "Fact Sheet Cyber Security", December 2017.

[9] ICAO, Assembly Resolution A39-19, September 2016.

[10] Thales UK Ltd, "White paper - Cyber Security for SCADA Systems", 2013.

[11] ENISA, "Baseline Security Recommendations for IoT", 2017.

[12] ENISA, "Communication network dependencies for ICS SCADA Systems", December 2016.

[13] S. Sachchidanand, S. Nirmala, "Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce", International Conference on Green Computing and Internet of Things, IEEE, 2015.

[14] A. Abdullah, H. Al-Sakran, "Smart Airport Architecture Using Internet of Things", Intern. Journal Innov. Research in Comp. Science & Technology, Vol. 4, September 2016.

[15] G. Stergiopoulos, E. Vasilellis, G. Lykou, P. Kotzanikolaou, D. Gritzalis, "Critical Infrastructure Protection tools: Classification and comparison", International Conference on Critical Infrastructure Protection, USA, March 2016.