PROFESSIONAL PAPER

Annals of Disaster Risk Sciences

Vol 3, No 1 (2020): Special issue on cyber-security of critical infrastructure

Airports' Crisis Management Processes and Stakeholders Involved

Vasiliki Mantzana, Center for Security Studies (KEMEA)
Eftichia Georgiou, Center for Security Studies (KEMEA)
Ioannis Chasiotis, Center for Security Studies (KEMEA)
Ilias Gkotsis, Center for Security Studies (KEMEA)
Tim H. Stelkens-Kobsch, Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)
Vasileios Kazoukas, Center for Security Studies (KEMEA)
Nikolaos Papagiannopoulos, Athens International Airport S.A (AIA)
Anastasios Nikas, Athens International Airport S.A (AIA)
Filippos Komninos, Athens International Airport S.A (AIA)

Address for correspondence: Vasiliki Mantzana, enter for Security Studies (KEMEA), Athens, Greece, e-mail: v.mantzana@kemea-research.gr

Abstract

Airports are exposed to various physical incidents that can be classified as aviation and non-aviation related incidents, including terrorist attacks, bombings, natural disasters (e.g. earthquake or tsunami and man-made disasters such as terrorist attacks) etc. (Kanyi, Kamau, & Mireri, 2016). In addition to this, cyber-attacks to airport operations are emerging especially with the increasing use of Information Systems (IS), such as electronic tags for baggage handling and tracking, remote check-in, smart boarding gates, faster and more reliable security screening technologies and biometric immigration controls etc. Any physical or cyber incident that causes loss of infrastructure or massive patient surge, such as natural disasters, terrorist acts, or chemical, biological, radiological, nuclear, or explosive hazards could affect the airports' services provision and could cause overwhelming pressure. During the crisis management, several stakeholders that have different needs and requirements, get involved in the process, trying to cooperate, respond and support recovery and impact mitigation. The aim of this paper is to present a holistic security agenda that defines the stakeholders involved in the respective processes followed during the crisis management cycle. This agenda is based both on normative literature, such as relevant standards, guidelines, and practices and on knowledge and feedback extrapolated from a case study conducted in the context of the SATIE project (H2020-GA832969). In meeting paper's aim, initially the normative review of the phases of the crisis management cycle (preparedness, response, recovery and mitigation) in the context of airports as well as general practices applied, are presented. Moreover, the key airport stakeholders and operation centres involved in airports operations, as well as during the crisis management are analysed. By combining the information collected, a holistic cyber and physical crisis management cycle including the stakeholders and the relevant processes are proposed. The crisis management process is taken into consideration into the SATIE project, which aims to build a security toolkit in order to protect critical air transport infrastructures against combined cyber-physical threats. This toolkit will rely on a complete set of semantic rules that will improve the interoperability between existing systems and enhanced security solutions, in order to ensure more efficient threat prevention, threat and anomaly detection, incident response and impact mitigation, across infrastructures, populations and environment.

Keywords

Airport, Crisis management process, Stakeholders

1. Introduction

Air Transport is one of the infrastructures that need to be protected, due to its criticality for the society. Airports, being Critical Infrastructures (CIs) that belong to this subsector, play a key role in people and goods transportation, as well as in regional, national and international trade. Along the years, more and more people use airplanes as a frequent mean of transport. As stated in SESAR project PJ04 (SESAR, 2018) 7.2 billion air travelers are expected by the International Air Transport Association (IATA) to travel in 2035, while this number in 2016 was cut close to half (3.8 billion).

Airports are one of the Critical Infrastructures where federal responsibility for overseeing and controlling air traffic operations intersects with local governments that own and operate most airports. Airports incorporate in their agenda passenger comfort, cost-efficiency, environmental protection and policies for corporate and social responsibility. It has been reported that airports are exposed to various physical threats that can be classified as aviation and non-aviation related, including terrorism, Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE), technological accidents, natural disasters, etc. (Kanyi, Kamau, & Mireri, 2016). In addition to this, cyber-attacks to airport operations are emerging especially with the increasing use of IS, such as electronic tags for baggage handling and tracking, remote check-in, smart boarding gates, faster and more reliable security screening technologies and biometric border controls etc.

It appears that it is fundamental for every airport to remain resilient, maintain the level of provided services, and be able to scale up its service delivery in any given emergency. Depending on the type of attack, airports aim to increase their capacity in order to respond effectively. Airport capacity, operations management and flight scheduling are vital elements for ensuring airports resilience. In the case of man-made disasters, such as bio-terror attacks or chemical release events the main aim of an airport is to minimize the number of deaths and the proper decontamination of victims in order to prevent other people in and out of the airport getting infected (Levent, K., Turan, K., Mehmet, E., Mesut, O., Hakan, Y., 2007). Based on literature findings a multidisciplinary approach among emergency medical services and airport authorities should be in place. Additionally, exhaustive safety and security plans, detection equipment and personal protective equipment for the first responders are among the minimum requirements in order to face such threats.

The management of a crisis does not start when the crisis occurs. The planning and coordination for response to any type of incident must be performed well in advance of an actual event. Crisis management has been defined as "the developed capability of an organization to prepare for, anticipate, respond to and recover from crises" (British Standard Institute (BSI), 2014). The full cycle of crisis management can be described in four phases: Preparedness aims to prepare airports and CIs in general to deliver an appropriate response in any crisis and mitigate the impact. Granted, that it is not possible to mitigate completely against every hazard, preparedness actions can facilitate response and recovery operations and reduce the impact. Response pertains to the adoption and implementation of emergency actions to save lives and property such actions might include building evacuation, restoring critical services, offering medical health, etc.. Recovery, aims to return the systems and activities to normal operations and protect the organization against future hazards and finally, mitigation includes those actions that will reduce or eliminate long-term risk to people and property from hazards and their effects.

The concept of the cycle implies an ongoing process which tries to eliminate disruptions, to provide immediate assistance to affected ontologies, to reduce disaster losses and to improve the conditions of the affected communities. Usually, the crisis management cycle is triggered by an event and begins with the response to that event. As the main aim is to respond to the specific threat, crisis management programs often prioritize the preparedness and response phases, leaving limited resources to address recovery and mitigation.

2. Problem analysis

A plethora of security measures are adopted in airport infrastructure to maintain the physical and cyber security of the passengers. However, there are still some gaps, and these are very representative of today's challenges in cyber and physical security of the airports. A key element in successful crisis management is comprehensive situational awareness among all stakeholders involved. Situation awareness is the perception of environmental elements and

events with respect to time or space, the comprehension of their meaning, and the projection of their future status (Endsley, 1995).

Taking into consideration the findings from SATIE workshops, reports of major national emergencies and disasters, and the daily challenges faced by the airports, the following gaps have been identified:

- Decentralised control and collection of information
- Lack of fast communication and information dissemination
- Overhead in expedient decision making
- Challenges with initial activities on arrival at scene
- Lack of common joint operational and command procedures
- The complexity of predicting the potential impact of a crisis i.e. fire propagation, , impact of toxic chemicals, radioactivity, cascading effects, etc.

It is crucial for airports to have a holistic physical and cyber crisis management process that explains how internal and external stakeholders cooperate and exchange information in a unified manner. In addressing this need, in the following paragraphs, a holistic physical and cyber crisis management process is presented. The stakeholders involved are identified and analysed and their interactions in the four concurrent and continuous crisis management phases (preparedness, response, recovery and mitigation) are presented.

3. Airports' crisis management stakeholders

During the crisis management, several stakeholders that have different needs and requirements, get involved in the process, trying to cooperate, respond and support recovery and impact mitigation. Security stakeholders can be categorized according to their involvement and perceived proximity to the organization into internal and external.

For the needs of the crisis management analysis to follow, the definition of internal stakeholders refers to the individuals and parties belonging directly to the organisation/airport while externals stakeholders represent parties which are outside the organisation and affect or get affected by the organisation's activities. Based on relevant literature review and information collected from the participating airports, the following list summarises the internal stakeholders in the context of SATIE (non-exhaustive list) (European Union Agency for Network and Information Security (ENISA), 2016) (National Academies of Sciences E. a., 2016) (National Academies of Sciences, 2015):

1. Airport's Board of Directors (ABoD)
2. Data Protection Officer (DPO)
3. Airport Duty Officer (ADO)
4. Physical security manager / personnel
5. IT Security manager / personnel
6. Technical manager / Technical staff
7. Crisis Management Centre (CMC) / Crisis Management Team (CMT)
8. Airport Operations Centre (AOC)
9. Emergency Operations Centre (EOC) /Emergency Operations Team (EOT)
10. Security Operations Centre (SOC) /Security Services Department
11. IT department
12. Media centre
13. Friends and relatives assistance centre

Before, during and after a crisis and in order to more efficiently and effectively handle incidents, internal stakeholders should cooperate and exchange information with external ones. The external stakeholders to be considered in the context of SATIE (non-exhaustive list) are the following:

14. International and EU Organisations (e.g. ICAO, EASA, EUROCONTROL)
15. Air Accident Investigation and Aviation Safety Board (AAIASB)
16. National Civil Aviation Authority (CAA) / Aviation Authority
17. General Secretariat for Civil Protection (GSCP)

18. National Authorities
19. National Intelligence Agency
20. National Data Protection Authority
21. Law Enforcement Agencies (LEAs) (e.g. Police)
22. Rescue Fire Fighting Services (RFFS)
23. Emergency medical services (ambulance) / First aid services
24. Air Traffic Control (ATC) (e.g. ENAV)
25. Interconnected / Interdependent Critical Infrastructures (e.g. metro/bus, refueling corporation, hospitals, power/gas suppliers, communication suppliers)
26. Information Security Service Providers
27. Telecommunication Providers
28. Airlines, Ground Handlers, Cargo
29. Concessionaires
30. Security and safety teams
31. Passengers

4. Holistic physical and cyber crisis management process

The airport's crisis management process as well as the stakeholders involved in each phase (prepare, respond, recover and mitigate) are presented in the following subsections. The mentioned steps in the following text refer to Figures 1 and 2 at the end of this chapter.

Preparedness phase

Preparedness is a continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective actions that internal and external stakeholders should follow closely to ensure organization readiness. For an airport to prepare for crisis management, it is important to know which assets are vital for conducting its core activities, and which are the potential threats against these assets, as well as their vulnerabilities (step 1). Risk assessment constitutes the fundamental first step in preparedness and this means the identification and analysis of major threats, hazards and related vulnerabilities. In addition, appropriate institutional structures, clear mandates supported by comprehensive policies, plans and legislation and the allocation of resources for all these capacities through regular budgets are also instrumental for thorough preparedness to crisis. The Crisis Management Plan (CMP) is a document that mostly sets out the following: i) persons in charge for key decisions and actions during a crisis, ii) the structure of the CMT, and representatives involved in this team, iii) updated main contact list and the ways the communications will be held in the event of a crisis, iv) the plans and mechanisms to be activated during a crisis and how they work in practice, v) flow charts specifying the sequence of actions and interactions and vi) definition of places for the CMT to meet, equipment and support required (Airport Cooperative Research, 2016). Once the CMP has been written, approved and tested, airports should make sure to review and update it frequently and as part of the post incident review, as employees join or leave the company, new technologies are implemented, and other changes occur. Based on the level of the crisis, there exist several national CMPs, which might be activated. These plans and procedures are part of the regulatory framework that the airports follow.

In addition, to improve the efficiency of the CMT the appropriate tools must be in place (step 2). The tools might include things from a contact list to hardware and software tools including intrusion detection systems, decision making tools, impact assessment tools, assets registration and criticality, risk analysis tools, simulation exercises, etc. The contact list should include contact details (e.g. address, telephone, email, back up contact info) of all those people that will help and collaborate during a crisis. Additionally, the CMT should make use of autonomous systems that can be used even when the organisation's systems or networks have been compromised. Last, but not least, training and exercising are the cornerstones of preparedness which focus on readiness of all involved actors to respond to any type of incidents and emergencies and on the identification of any discrepancies in terms of resources (step 3).

Response phase

Response initiates when an incident is detected by an internal or external stakeholder (e.g. SOC operated by an external organization) in a manual or automated way (e.g. monitoring networks and early-warning systems, public authorities, citizens, media, private sector, etc.) (step 4). Involved stakeholders should start gathering information that will be used for the initial assessment of the incident. Depending on the type of the incident (cyber or physical or their combination) different stakeholders will collect the information needed for further investigations. Additionally, information from multiple sources, such as social media and crowdsourcing could be collected. The physical security manager, the IT security manager, and the technical manager should initiate the process. The SOC and the IT department, as well as the external stakeholders such as the law enforcement agencies, the RFFS, the interconnected critical infrastructures, the external security and safety teams, and the airlines and ground handlers could participate in this step. The information to be gathered usually includes details relevant to the type of incident, the present hazards, the access-routes that are safe to use, the number and the type of casualties (if any), meteorological information, geolocation information, images, video, the timestamps, the analysis, the cause, the status, the custom parameters, etc. (step 5). The information should be collected and assessed by the ADO in cooperation with relevant stakeholders that identified the incident (step 6). Based on the criticality of the incident, the Crisis or Emergency Management Team should be informed, triggered and coordinated by the ADO. The ADO with the support of the CMT should assess the extent of the crisis, evaluate the situation, determine, and define which response plan(s) should be activated (e.g. evacuation plan, etc.) and activate additional stakeholders to be involved, as deemed necessary. The ADO will also inform the ABoD, and the Media Centre (if needed). Depending on the stakeholders involved in the response phase (e.g. police, RFFS, etc.), different plans might be activated. Based on the activated plans, response processes and procedures are executed, coordinated and adapted. Disconnection, denial of remote access (i.e. VPN), isolation of affected systems, identification of root cause, and collection of logs could be some of the response actions to be followed (step 7); appropriate resources should be allocated and released, and actions should be assigned to stakeholders and tracked by the ADO, with the support of the CMT or EOC in case that it has been activated by the ADO. Moreover, it is crucial to know the location of responders and their proximity to risks and hazards in real time, as well as to monitor and analyse passive and active threats and hazards at incident scenes in real time (Homeland Security Studies and Analysis Institute, 2014) (step 8). In addition, the CMT is responsible for communicating in a timely, accurate and precise manner relevant information as collected in step 5 (that can be used for management, informative purposes), to internal and external stakeholders, in order to manage crisis and protect the brand and reputation of the organization by implementing relevant decisions (steps 9 & 10). Leadership plays a key role in crisis communication. Communicating with the media and the general public to provide a sense of events, to maintain trust in the emergency responders and government, and to transmit specific messages are essential functions of leaders during crisis. Particular attention should be paid to the reports' circulating during a crisis handling. A great number of reports by the participants in the CMC agencies/organizations will be required by pertinent internal directives of these agencies or may be requested by senior management. The CMT usually maintains a log of the crisis and sets out the report after the crisis termination.

The afore-mentioned steps could repeat, until resources return to their original use and status (demobilization) and crisis terminates. As a crisis winds down, CMT should clearly indicate closure to the relevant internal and external stakeholders through a formal, well-communicated process to help minimise anxiety and encourage the return to normality. All the internal and external stakeholders that participated during the response phase participate in this step as well (step 11).

Recovery phase

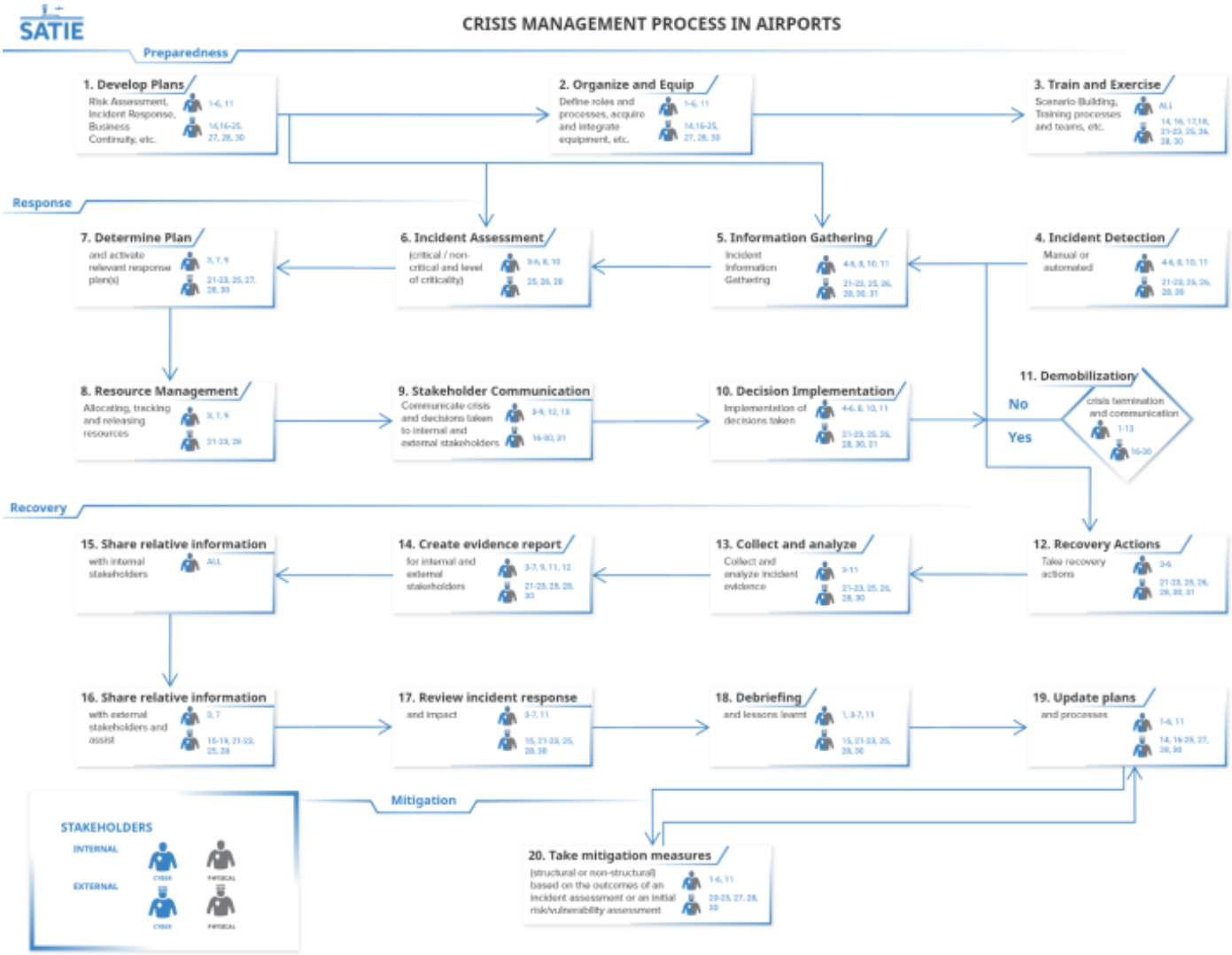
Recovery consists of those activities that continue beyond the emergency period to restore critical community functions and begin to manage stabilization efforts. This phase is executed during or after the response phase termination and is directly affected by decisions made as part of the previous phase. The CMT should decide the recovery actions to be taken (based on recovery plans), by coordinating closely with the ADO, the physical security manager and personnel, the IT security manager and personnel, the technical manager and staff, and the IT department in cooperation with external stakeholders depending on the type of crisis and the activated response plans (step 12). Moreover, the evidence from the incidence should be collected; analysed (step 13); and an evidence report should be created by CMT (step 14). CMT in cooperation with ADO should share relative information with all internal stakeholders (step 15) and external stakeholders and investigations should be assisted (step 16). Moreover, as crisis serves as a major learning opportunity for both internal and external individuals and organizations, should review the overall process as well as plans, procedures, tools, facilities etc., to identify areas

for improvement (step 17). Following the evaluation, lessons learnt should be identified (step 18) and recommendations / changes should be made to relevant plans and processes (step 19) by internal and external stakeholders (as described in step 1).

Mitigation phase

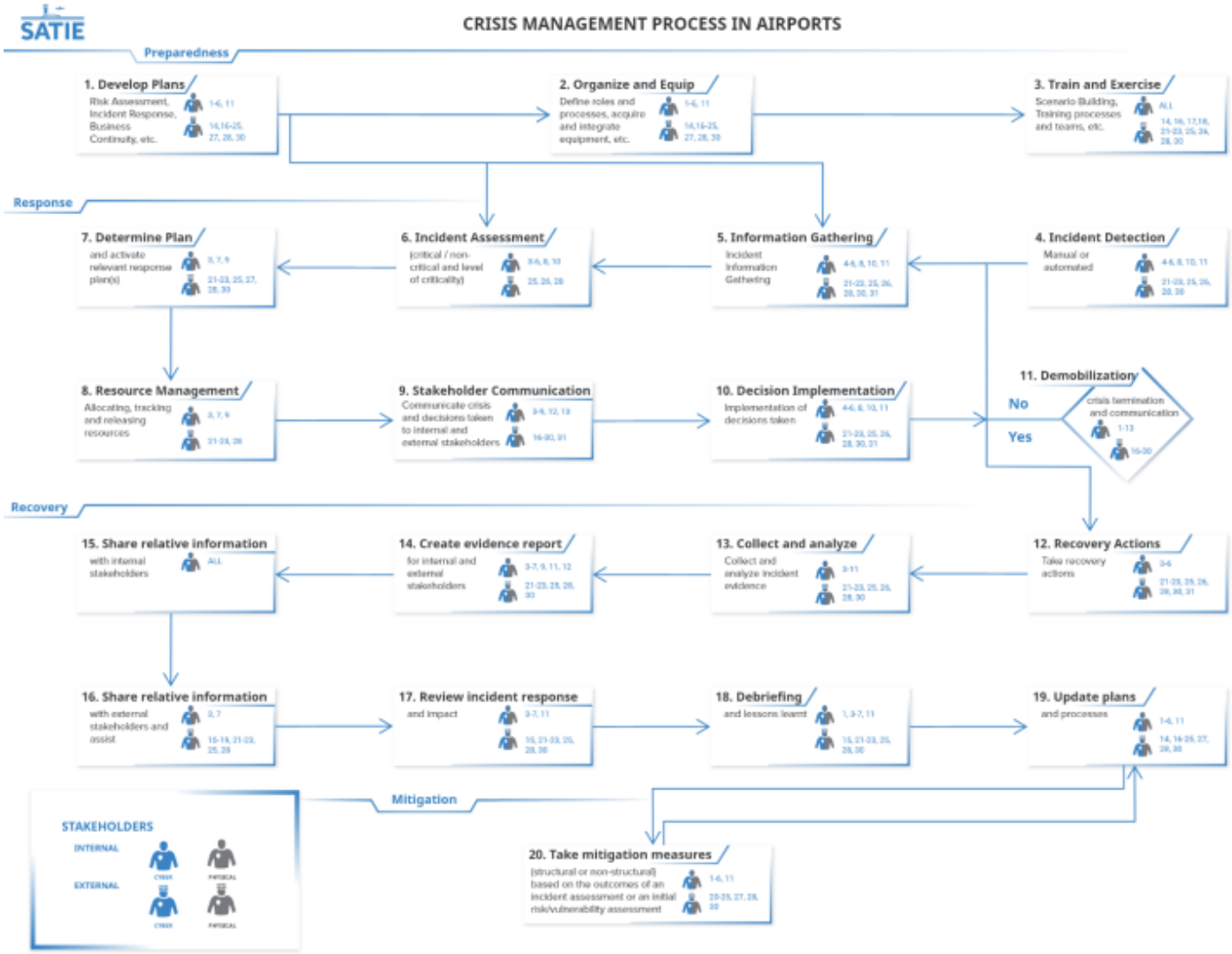
Lessons learned should be carried out for any crisis event. An airport or any type of organisation that has successfully been attacked should return to normal operations after new countermeasures have been implemented. Based on the outcomes of the incident consequences, some of the activities that previously were defined as normal will probably need to be revised. The results of the evaluation of the response actions should lead to recommendations for change, and responsibilities and timelines in order to ensure that it will be carried out (step 20). It is common, that discrepancies are identified but not actually addressed, resulting at the organization's disposal to future crises. Proposed changes might include organizational changes, structural (such as changing the characteristics of buildings; perimeter security etc.) and non-structural measures (adopting or changing physical and cyber access controls, training etc.).

The following figures summarise the phases of the airport's crisis management process as well as the stakeholders involved in each phase, as already described in the previous paragraphs.



Click for full size image

Figure 1. Common and holistic security and safety agenda (Preparedness and Response phases)



Click for full size image

Figure 2. Common and holistic security and safety agenda (Recovery and Mitigation phases)

5. Conclusions

The goal of this paper was the presentation of a holistic airports' crisis management cycle including the relevant stakeholders and processes. Taking into consideration the findings from SATIE workshops, reports of major national emergencies and disasters, and the daily challenges faced by the airports, areas for improvement have been identified. In this regard, the holistic security/safety agenda being ultimately proposed by SATIE provides for setting the common ground among all stakeholders in managing a crisis thus reducing administration/coordination overhead and enhancing the process of efficient decision making.

As it has been highlighted, during a cyber and/or physical incident, different categories of stakeholders either internal or external might be fundamentally affected when an airport's routine operations are compromised and disrupted. The crisis management is an extensive procedure, and the interactions among the numerous stakeholders can be very complex. Situational awareness and information sharing have been recognized as a critical foundation for successful incident response and decision-making activities during the crisis management process. Having a shared situational awareness, the various stakeholders involved in the crisis management collaborate more

efficiently to the crisis resolution. Emergency procedures can be triggered simultaneously through an alerting system in order to reschedule operations, notify stakeholders including first responders, cyber/physical security and maintenance teams towards a fast and effective response and recovery The common cyber-physical crisis management process suggested to be followed by airports and CIs, at Member States level, aims to set common ground among stakeholders in managing incidents, thus reducing administration overhead and enhancing the process of efficient decision making and information sharing, including best practices and lessons learned. Thus, this paper offers a broader understanding of the CIs' security management.

Acknowledgements

The work presented in this paper has been conducted in the framework of SATIE project, which has received funding from the European Union's H2020 research and innovation programme under grant agreement no. 832969. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

References

Kanyi, P., Kamau, P., & Mireri, C. (2016). Assessment of the appropriateness and adequacy of the existing physical infrastructure in mitigating aviation risks at Wilson Airport, Kenya. *IOSR J. Humanit. Social. Sci.*, pp. 51-62.

SESAR. (2018). Periodic Reporting for period 2 - PJ04 TAM (Total Airport Management).

Endsley, M. (1995). A taxonomy of situation awareness errors, human factors in aviation operations. *21st Conference of the European Association for Aviation Psychology (EAAP)*, (pp. 287-292).

Airport Cooperative Research. (2016). *Emergency Communications Planning for Airports.*Washington, DC: The National Academies Press.

British Standard Institute (BSI). (2014). *BS11200: Crisis Management – guidance and good practice.* London, UK: BSI.

European Union Agency for Network and Information Security (ENISA). (2016). *Securing Smart Airports.* Retrieved from ENISA: https://www.enisa.europa.eu/publications/securing-smart-airports

Homeland Security Studies and Analysis Institute. (2014). *Project Responder 4: 2014 National Technology Plan for Emergency Response to Catastrophic Incidents.* Retrieved from https://www.hsdl.org/?view&did=764107

Levent, K., Turan, K., Mehmet, E., Mesut, O., Hakan, Y. (2007). Chemical release at the airport and lessons learned from the medical perspective. *J. Hazard. Mater., 144*, pp. 396–399.

National Academies of Sciences, E. a. (2016). *Emergency Communications Planning for Airports.* Washington, DC: The National Academies Press.

National Academies of Sciences. (2015). *Guidebook on Best Practices for Airport Cybersecurity.* Washington, DC: The National Academies Press.