Turkish Studies
International Periodical for the Languages, Literature and History of Turkish or Turkic
Volume 12/32, p. 33-48
DOI Number: http://dx.doi.org/10.7827/TurkishStudies.12682
ISSN: 1308-2140, ANKARA-TURKEY

Article Info/Makale Bilgisi
Referees/Hakemler: Doç. Dr. Murat ERTUĞRUL – Yrd. Doç. Dr. Gökdeniz KALKIN – Yrd. Doç. Dr. Devrim GÜN

This article was checked by iThenticate.

INVESTIGATING CRITICAL POINTS OF CYBER SECURITY: PREVENTION TERROR ATTACKS IN AIRPORTS*

*Savaş Selahattin ATEŞ** - Haşim KAFALI*** - Mevlüt ÜZÜLMEZ**** - Hasan LIK*****

ABSTRACT

Airports are one of the most developed structures in point of electromagnetic and digital information aspect. Extremely high amount of information about aviation operation has to be connected with all related units in order to keep operation effectively on-time. Thus, communication web must be both reasonable punctual and well-protected. Since airports are equipped by millions system, it is quite essential to pick the right component to examine in order to find out the main points of system and to restore for the best security service level. At the end of this implementation, the potential failure types of critical points of airport have been examined and identified. So that in case of any cyber action, users will have been informed by the knowledge of proactive support system. Moreover, user will also be educated about how to react to prevent or minimize the possible damage coming from a cyber-attack. In the first stage of this paper, the theoretical researches of cyberspace and possible threats have been examined. In the second part, cyber security terms and units related to government policy have been stated. In the final part of the study, the categorization of possible cyber-attacks against airport systems have been discussed and evaluated by confidentiality, integrity, accessibility scale. To analyze failure type and level of its effect FMEA (Failure Mode Effect Analysis) method has been applied in this study. This method is one of the strongest numerical

* This study was supported as part of project *Decision Support System for Flight Planning in Flight Training Organizations: Application in Anadolu University Faculty of Aeronautics and Astronautics* accepted by the Commission on Scientific Research Projects, Anadolu University.

** Yrd. Doç. Dr. Anadolu Üniversitesi Havacılık ve Uzay Bilimleri Fakültesi Havacılık Yönetimi ABD, El-mek: ssates@anadolu.edu.tr

*** Yrd. Doç. Dr. Muğla Sıtkı Koçman Üniversitesi Dalaman Sivil Havacılık Yüksekokulu Sivil Havacılık ABD, El-mek: hasimkafali@mu.edu.tr

**** Arş. Gör. Erciyes Üniversitesi Havacılık ve Uzay Bilimleri Fakültesi, Sivil Havacılık ABD, El-mek: mevlutuzulmez@erciyes.edu.tr

***** Öğr. Gör. Anadolu Üniversitesi Havacılık ve Uzay Bilimleri Fakültesi, Sivil Havacılık ABD, El-mek: hlik@anadolu.edu.tr

techniques which prevent failures before they even exist and identify how to convert high risk components into reliable factors. With analyzing the obtained results, a system which is aimed to be used in Atatürk Airport for scaling and taking considerable proactive actions have been identified and on the purpose of improvement of system some recommendations have been made.

STRUCTURED ABSTRACT

Purpose: Research carried out within the scope of the airport cyber security. Changing life, technology and society conditions are leading to a shift in security perspective. While the number of electronic-based systems and virtual platforms that people and businesses use has increased, security needs and threats have changed accordingly.

Design/Methodology/Approach: In this study, the failure type and level of its effect FMEA (Failure Mode Effect Analysis) method is used to analyze and investigate on critical points of airports cyber security. This method is one of the strongest numerical technique which prevent failures before they even exist and identify how to convert high risk components into reliable factors. In the scope of this research, firstly literature search related to cyber security has been done. In the second part of the study, measures taken by the state on cyber threats in public areas such as airports are explained. In the last part, a FEMA scale was developed which consisting three airport-relating steps. In the first dimension of the scale, the systems in the airports were analyzed with the help of literature research. A list of weak systems against cyber threats has been tried to be created. However, due to the unique nature of each airport, a questionnaire form was developed for each employee. The developed questionnaire forms the first dimension of the scale. The second dimension of the scale consists of face-to-face interviews. Face-to-face interviews determine the order of importance of airport systems. In the third dimension of the scale, Likelihood of Occurrence, Discoverability, Severity Scale and Confidentiality, Integrity, Accessibility Scale are assigned to the airport to determine the effect of probable cyber-attacks on the airport. It is planned that the scale developed in the survey will be applied at airports.

Findings/Results/Discussion: Airport systems and their threat level in terms of cyber security is identified with the framework of ISO 27001. Concept of cyber security is explained and the important information assets in terms of cyber threats in Airport Systems are defined. End of the research decision tree diagram which shows the steps of discoverability, the severity scale has been formed.

People have felt the need to take measures against the elements that threaten them for years. Security is one of the most basic needs of an individual or an enterprise. Therefore, security is in the class of necessities. Changing life, technology and society conditions are leading to a shift in security perspective. While the number of electronic-based systems and virtual platforms that people and businesses use has increased, security needs and threats have changed accordingly.

In general, it is necessary to determine the systems used in an airport. These systems vary depending on the size and structure of the

airport. At least one unit manager should be contacted from all the units in the organization chart of the airport. Airport inventory should be overlooked. If airport systems are exposed to cyber terrorism, to determine the critical points of airport systems, possible effects should be taken orally and the systems should be ranked according to their importance. In the event of a possible cyber-attack on airport systems, the confidentiality of the information may be violated. Systems should be questioned for privacy reasons. However, in terms of integrity (unauthorized modification / incorrect replacement) each system should be evaluated. Airport critical systems should be questioned in terms of accessibility / availability.

Research Limitations/Implications: Airports make hosting more than one systems. For this reason, there are many systems used in airports. The scope of the research is limited only to the systems under control of the airports. The systems used by other airport operators are not included in the survey. For example, the systems that ground services using have been ignored.

Practical Implications: A FEMA scale was developed which consisting three airport-relating steps. It is planned that the scale developed in the survey will be applied at airports. A warning has been received that the sharing of this application by many airports would constitute a significant security breach when scales were sent to airports. With analyzing the obtained results, a system, which is aimed to be used in Atatürk Airport for scaling and taking considerable proactive actions, have been identified. On the purpose of improvement of system some recommendations have been made.

Social Implications: Airports are one of the important sub-structures of aviation millions of the people use airport system to transportation. With the developed system airports companies can investigate on cyber security of the airport systems

Originality/Value: The airports are under the threat of terrorist organizations for economic, socio-cultural and political reasons. Physical security threats have begun to evolve into threats in the virtual platform due to changing ways of doing business. It is thought that with this research, airports including current social, economic and cultural dynamics of the countries, make significant contribution to academic literature and will also include security analysis by presenting findings.

Keywords: Cyber security, Cyber-attacks and threats, Airport security, Airport cyber security systems, Proactive actions against cyber-attacks.

SİBER GÜVENLİKTE ÖNEMLİ NOKTALARIN İNCELENMESİ: HAVAALANLARINDA TERÖR SALDIRILARININ ÖNLENMESİ

ÖZET

Havaalanları elektromanyetik ve dijital bilgi açısından en gelişmiş yapılardan biridir. Etkin ve zamanında operasyonun sürdürülebilmesi için ilgili havacılık operasyon birimlerindeki yüksek miktardaki bilginin birbirlerine bağlanması gerekmektedir. Dolayısıyla, iletişim ağı hem

makul, hem de iyi korunmuş olmalıdır. Havaalanları milyonlarca sistemle donatılmış olduğundan, sistemin ana noktalarını bulmak ve en iyi güvenlik hizmeti seviyesini geri yüklemek için inceleyecek doğru bileşeni seçmek esastır. Bu uygulamanın sonunda, havaalanının kritik noktalardaki olası hata türleri incelenecek ve tanımlanacaktır. Dolayısıyla, herhangi bir siber eylemin olması durumunda, kullanıcılara proaktif destek sistemi bilgisi verilecektir. Ayrıca, kullanıcılar bir siber saldırıdan kaynaklanabilecek muhtemel zararları önlemek veya en aza indirmek için nasıl tepki vereceği konusunda eğitilecektir. Makalenin ilk bölümünde, siber yapı ve muhtemel tehditler kuramsal olarak incelenmiştir. İkinci bölümde hükümet politikasıyla ilgili siber güvenlik şartları ve birimler belirlenmiştir. Çalışmanın son bölümünde havaalanı sistemlerine karşı olası siber saldırıların sınıflandırılmasında gizlilik, bütünlük ve erişilebilirlik ölçeği ile ele alınmış ve değerlendirilmiştir. Bu çalışmada, hata tipini ve seviyesini analiz etmek için FMEA (Hata Türleri ve Etkileri Analizi) yöntemi uygulanmıştır. Bu yöntem, hata belirleme ve önleme için en güçlü sayısal tekniklerden biridir ve yüksek riskli bileşenlerin güvenilir faktörlere dönüştürülmesini sağlar. Elde edilen sonuçları analiz ederek Atatürk Havalimanı'nda ölçeklendirme ve önemli proaktif eylemler için kullanılması planlanan bir sistem belirlenmiş ve sistemin iyileştirilmesi amacıyla bazı öneriler yapılmıştır.

Anahtar Kelimeler: Havacılıkta siber güvenlik, Siber saldırılar ve tehditler, Havaalanı güvenliği, Havalimanı siber güvenlik sistemleri, Siber saldırılara karşı proaktif eylemler.

Introduction

Information forms the basis of all intuitional operation and appears almost at every step of process. It can be on both physical and digital environment as paper or e-mail etc. Especially with the development of information technology, most of information becomes important for the institution at low or high level which should be protected from physical and cyber threats. For that reasons organizations have been looking for comprehensive and effective protection against those threats.

Digitalized information has been dominant in all departments since computer became more available and practical for communication in the Internet technologies. Therefore, securing the cyber environment has also become one of the major agenda for information technology units. Not only for institutional level but also for the government, cyber-security policy is getting more essential so that security policies had been developed with the innovation in cyber space. Providing corporate information security is a dynamic process and it is an ongoing process. It must be done and implemented in accordance with international standards (Doğantimur, 2009). When risk level of organization is considered, airports are extremely crucial for the country which is used as a gate to outer world. Thus, infrastructure of intellectual property at the Airports must be kept highly secured against any kind of illegal and malicious attacks. Airports are consisted of thousands of different systems from tower-plane communication to the terminal boards. Each one has their own transfer program codes and stock databases. So that, cyber security practices are getting in upper hand in those fields in order to minimize possible attacks which may affect flight safety directly or indirectly. One of the critical infrastructures identified and approved by the Cyber Security Council is the Transportation Sector (Computerhope, 2016). Since the aviation sector is a sub-sector of transportation and it has a critical infrastructure, it is foreseen to establish Sectoral SOME within the

scope of our General Directorate. SOMEs are obliged to take necessary precautions against direct or indirect sabotage against the affiliated organizations of the sector and to establish mechanisms and event recording system that can interfere with such events (Havacılık Güvenliği Daire Başkanlığı, 2016).

In this paper, it is aimed to identify airport systems and their threat level in terms of cyber security. Secondly, determination of their risk level with confidentiality, integrity, accessibility scale and possible result has been evaluated. Finally, a decision tree diagram which shows the steps of discoverability, the severity scale has been formed.

Literature Review

Recently, rapid development of digital technology is playing an important role in many sector including information and communication which are affecting our life directly. The transition from analog equipment to digital equipment brings a number of benefits, as much as new kind of problem (Jinsoo Shin, 2016). Nowadays, information technologies have been very common at many levels such as personal, institutional, systemic occasion. It involves individual and a global level of work related to digital environment (Aydın, 2012). There are several way of describing cyberspace, these are only two of them: [1] *Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. In effect, cyberspace can be thought of as the interconnection of human beings through computers and telecommunication, without regard to physical geography* (TechTarget, 2016). [2] "*The notional environment in which communication over computer networks occurs"* (Oxforddictionaries, 2016). "*Cyberspace is fictitious, instead of real and perceivable stage. Old and standard definition showed that the experience of cyberspace was completely different from that of previous explained spaces*" (Lee et al., 2002).

Threats in Cyberspace

All kind of different attacks aim to damage or to take advantage of people, government, data, application or system basically (Aydın, 2012). Every system has a protection even if it is a lock or anti-malware software yet human factor is always occasion for attacker to get into what is protected (Lord, 2012). That is the reason although system has protection in full, there will always be a gap to leak in. Cyber attackers could use both user and system shortage in order to break protection (Islam, 2010; Tosun, 2016). Cyber treat can be explained by the definition of "*A **cyber threat** is deemed any malicious act that attempts to gain access to a computer network without authorization or permission from the owners* (Wert, 2016; Park, 2010)."

Cyber Terrorism: Hence it is fairly new concept, there are multiple statement about cyber. Through all of explanation, FBI define it as: "*...any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."*

Government Role in Cyber Security

Cyber technology is one of the most important developments for both company and country recently. Intellectual capital is taking a huge part in communication and coordination among companies and individuals. In order to improve power and capacity of cyber security, countries must increase cyber-attack powers as well as security. Therefore, cyber security must be ensured at both governmental and operational level (Çeliktaş, 2016). A cyber-attack to the country or its organization is very critical for overall security. Every government may have some confidential information to plan and manage its sub-departments. That is the reason why these information needs to be kept secure in cyber space (Aydın, 2012). Especially with the spreading of information

technologies in most of the industries such as transportation, education, health, security services etc. cyber security becomes an importance in the modern world and it is one of the most important things to develop businesses and governments to higher priorities in order to follow the growth in this area. Cyber security has become popular recently due to the extensive use of digital I&C systems and the importance. The reason why cyber security exists is that it is protecting these systems against cyber infrastructure attacks planning to sabotage or eliminate the system (Jinsoo Shin, 2016). Threats can be run by different origin for example inside or outside based attacks. And results say that attacks which are originated from outside an organization are likely to have more different attack characteristics than internal threats. Therefore, companies may need to improve their security risk scenario and its possibilities (E Byres, 2004).

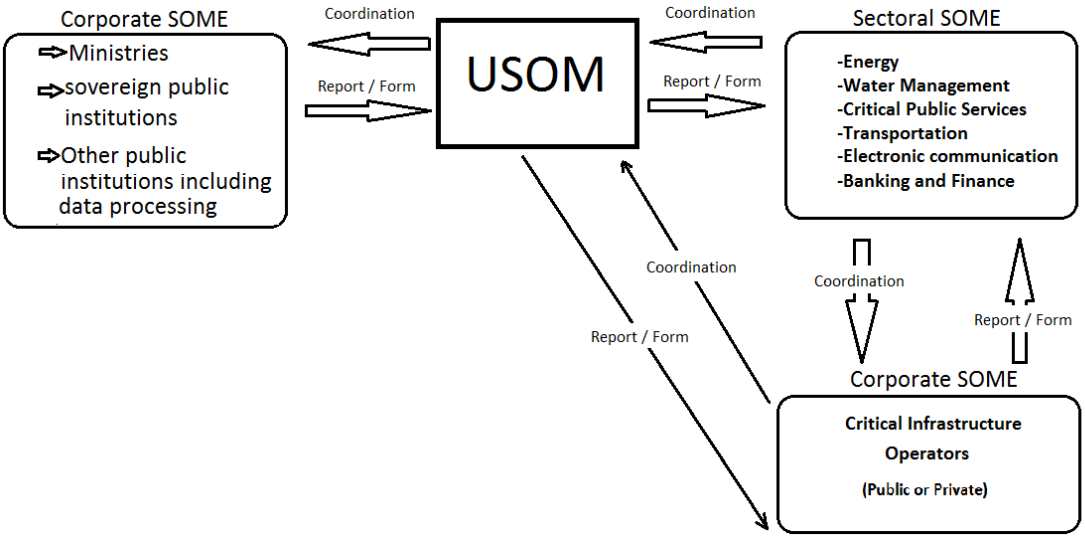
National Organization Against Cyber Actions

Most of countries have been developing administrative systems, technical and judicial environment to ensure cyber security across the country. With regards to this improvement, Turkey has published regulation. All cyber-security related infrastructures were accelerated. Moreover, National Intervention Centre Against Cyber Actions (USOM) has been founded on 27 May 2013 to coordinate and collaborate units on account of secure and effective process (SHGM, 2014). Turkey has declared a national organization against cyber actions both in private business which runs critical infrastructure and governmental institutes. There are three types of components of this organization: USOM, Sectoral SOME and Corporate SOME (Haberleşme Genel Müdürlüğü, 2014).

- **USOM (Ulusal Siber Olaylara Müdahale Merkezi):** USOM has been founded to interfere cyber actions country-wide and coordinate national and international information. It executes alarm against cyber security, warning, announcement operations so that controlling the national and international coordination is run under USOM (Bilgi Teknolojileri ve İletişim Kurumu, 2017). USOM is one of major actor of information technology and communication system which was generated to identify threats which exist in cyber space, decrease or destroy the impact of attacks (Ulusal Siber Olaylarla Müdahale Merkezi, 2017).

- **SOME (Siber Olaylara Müdahale Ekibi):** SOME is a team under control of USOM. This team is created to find quick and efficient solution to any kind of cyber-attack at first time and examining the way of block for potential new ones (Ulusal Siber Olaylara Müdahale Merkezi, 2017; Normatürk, 2017). Employees of SOME which is fighting against cyber-actions-information security specialist, system examiner, network specialist, network forensic officers and law enforcement agency should be taught about revealing system cracks and leaks, counter-action, leaking testing, attack methods etc. They also need to save reports into to system to gain awareness with malicious actions (Dijitalx.com, 2017). There are two types of SOME: sectoral and corporate SOME as Table 1.

Table 1 Relationship of USOM with Corporate and Sectoral SOME *(Bilgi Teknolojileri ve İletişim Kurumu, 2017)*



- **ISO 27001 Information Security Management System Standard**

ISO 27001:2013 Information Security Management System is a management system standard which is regulated and published by International Standardization Organization (ISO). Organizations support their business and operations with advanced technologies and software (databases, package programs, etc.). Thanks to these sub-structures, all activities and applications can be effectively controlled and managed. Information Security Management System (ISMS) standard is a management system designed to secure the security of information infrastructures, together with developing technologies. With the Information Security Management System, organizations determine information assets, analyze possible threats to these assets, and decide on actions to be taken if risks occur and actions to reduce the risks involved. This ensures that the confidentiality, integrity and accessibility of the information assets are guaranteed by minimizing the risks and impacts of the threats to the information assets. The ISO 27001 Information Security Management System has become an integral part of the integrated management system, especially for organizations moving towards institutionalization.

Cyber Security at Airports

Airports are huge environment involved with baggage-check services, check-in, border control and handling operations. Not only transportation services, but also customer related services (Wi-Fi, Tertapol, 3G/4G, Bluetooth etc.) are being offered all day long (Koç, 2008; Center, 2016). Therefore, keeping the system connected each other securely matters in case of sudden attacks. Communication among these units requires highly sophisticated information communication technology (ICT). Key factor to ensure this uncertainty is cyber-security to operate the airspace and mastermind inspections. All these possibilities prove that both air and land side of airport must be kept secured on cyber space to prevent any kind of negative condition (Gocen, 2015). Airports host passenger and cargo traffic which cause congestion at some point and especially in rush hour this capacity problem may bring information and communication system down (Ateş & Üzülmez, 2016$_a$).

Infrastructure of Intellectual Property at the Airports

Regarding technologic and social development, users of air transportation are growing and it leads a great deal of data input to the system (Ateş & Üzülmez, 2016$_b$). Aviation industry is heavily

relying on information and communication technology (ICT) to operate both their daily and seasonal actions. To represent basically, Figure 1 below shows the extensive infrastructure of ICT of Heathrow Airport Terminal-5 (Gramatica, Fabio Massacci (Member, Shim, Tedeschi, & Williams, 2015).

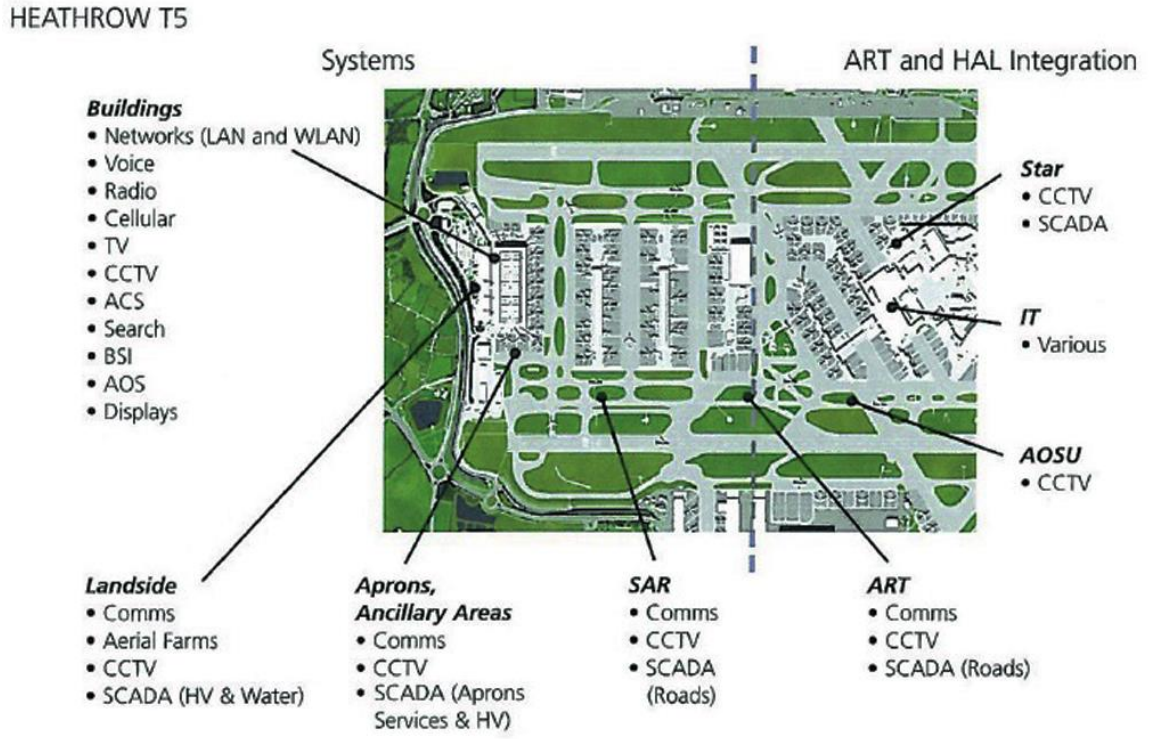


Figure 1 ICT services and devices used in Terminal 5 of Heathrow airport, U.K.

Firstly, in order to increase the capacity of airport and lessen the operation cost of all actions US uses NextGEN program as a ICT technology while EU is using SESAR. With the development of IT, IP-based-infrastructure -System Wide Information Management (SWIM)- is taking place of isolated system. SWIM helps to run overall operation more properly and punctual although it may need larger data stores to save and process more complicated information. Moreover, Remove and Virtual Tower (RVT) is another brand-new concept. Thanks to virtual reality and remote sensors, all the physical and remove control has left their places to new sophisticated systems which manage operation according to the information on their sensors. Though it looks pretty easy and handy, new cyber threats had started to pop out with this improvement of cost saving system (Gramatica, Fabio Massacci (Member, Shim, Tedeschi, & Williams, 2015).

Possible Proactive Solution of Cyber-Attacks at Airports

Both aerodrome and various companies run their operations through nested network webs including security and service systems. So that ensuring whole systems security may not be so easy like traditional business infrastructure. Attacks come out not only from direct way but also different web ways which are considered secure. Airports spread information to public by the Internet and to other business partners by local area networks. That is the reason why there is no specific one threat point. Each communication web must be examined and secured on its own and information flow should be processed via one-way air well by means of physical isolations (Herdem, 2017). Since there are number of services that completely open-access to the Internet, airport internal

infrastructure must be separate from those services. Backbone system could be weak against external attacks because any action may connect to internal data. Because even low-qualified hackers may commit an attack such as DDoS (Willson, 2016; Yagoda, 2014). Biometric screening methods (finger prints, face recognition) match the information with passport data to provide integration and secure spot. In addition, each user can be monitored at every point they proceed (Herdem, 2017). Otherwise, investing too little on cyber-security system may result with unacceptable level of risk which has severe consequences (Miller, Wagner, Aickelin, & Garibaldi, 2016).

On the other hand, system should not mistakenly believe that the attack always comes from outside. Firstly, Access of information systems should be gradual as much as possible in case any sort of sabotage actions. Secondly, role-based control system must be in force at critical points and finally with sensitive operations, at least two people acknowledgements must be taken before applying an action (Herdem, 2017).

Data and Methodology

The dependence on information technology is growing day by day, both as an individual and as an institution. For this reason, today's works have been carried out with technological infrastructure. Organizations support the information infrastructure with advanced hardware, databases. Airports are one of the aviation sub-structures used by millions of airline passengers and staff during the year (Gandotra, 2014). In recent years, international terrorist organizations have chosen airports as a focus. One of the methods used by contemporary terrorist organizations is cyber terrorism. The research is a theoretical work on the risks and effects that may arise in airports in case of a possible cyber-attack on airport systems.

The objective of the study is to develop the FMEA scale to be used in the analysis of the assets of the Airport Systems (Taş ve Koç, 2017).

Sub-research questions of the research:

- Question 1. What is the concept of cyber security?
- Question 2. What are the systems that governments and corporations apply to the provision of cyber security?
- Question 3. What are Airport Existing Systems?
- Question 4. What is the order of importance of airport existing systems in terms of cyber threat?
- Question 5. What are the important information assets in terms of cyber threats in Airport Systems?
- Question 6. How is the Discoverability, the Severity Scale applied in the airport systems?
- Question 7. How is the Confidentiality, Integrity, Accessibility Scale adapted to airport systems?
- Question 8. How should the FMEA scale be for asset analysis of airport systems?

Developed scale will shed light on the development of measures, assessing the risks of the airports against potential cyber terror incidents and solutions to priority risk points and the assessment of risks (Cesare, 2010). Secondary data analysis method (Literature search) and face to face interview was used in the research.

Findings and Discussions

Design of Scale Development Steps to Determine Airport Cyber Attacks

In the first dimension of the scale, the systems in the airports were analyzed with the help of literature research. A list of weak systems against cyber threats has been tried to be created. However, due to the unique nature of each airport, a questionnaire form was developed for each employee. The developed questionnaire forms the first dimension of the scale.

The second dimension of the scale consists of face-to-face interviews. Face-to-face interviews determine the order of importance of airport systems. In the third dimension of the scale, Likelihood of Occurrence, Discoverability, Severity Scale and Confidentiality, Integrity, Accessibility Scale are assigned to the airport to determine the effect of probable cyber-attacks on the airport (Figure 2).

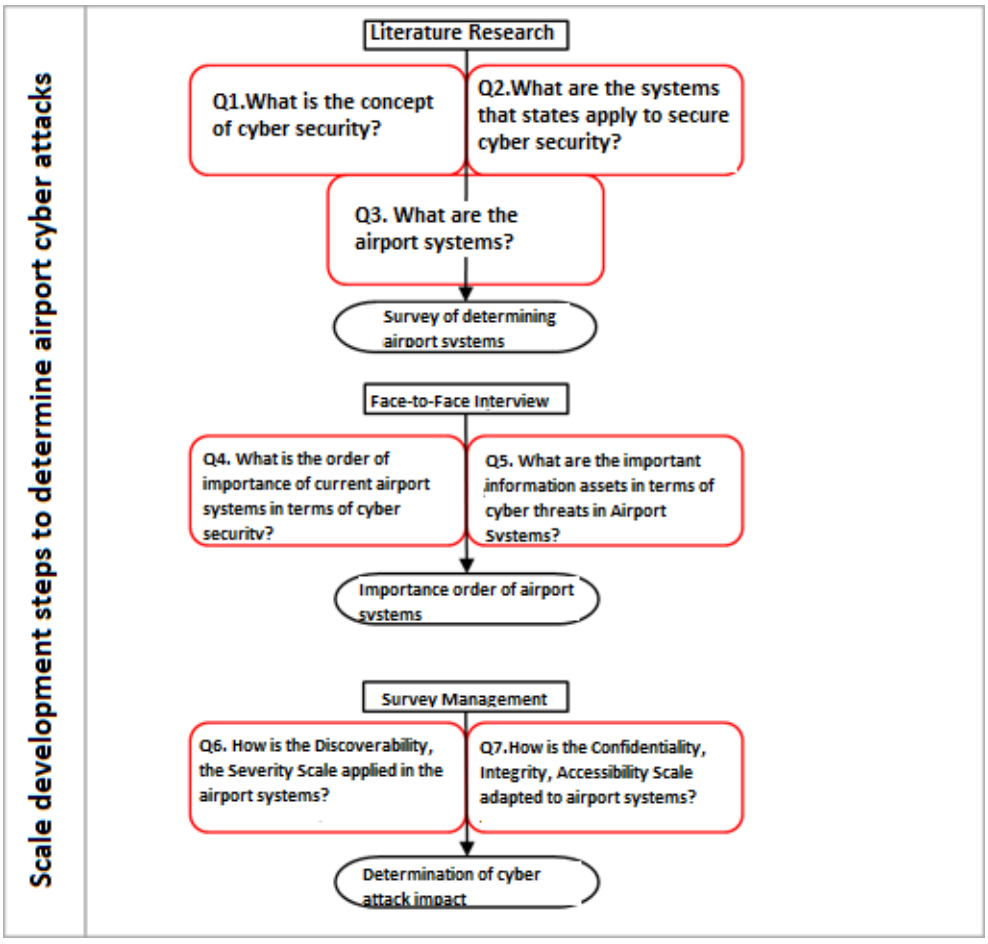


Figure 2 Steps to Determine Airport Cyber-Attacks.

Determination of Airport Systems

In general, it is necessary to determine the systems used in an airport. These systems vary depending on the size and structure of the airport. At least one unit manager should be contacted from all the units in the organization chart of the airport. Airport inventory should be overlooked. If airport systems are exposed to cyber terrorism, to determine the critical points of airport systems, possible effects should be taken orally and the systems should be ranked according to their

importance. Below are some of the critical systems that need to be questioned cyber terrorism in terms of the cyber-attacks in an airport within the scope of the literature survey (Table 2).

Table 2 Critical Systems in an Airport

TERMINAL ELECTRICAL TECHNICAL MAINTENANCE
Electric & Generator System
Chiller Plant (air conditioning)
ECBS (Emergency Case Battery System)
Lighting
UPS (Uninterruptible Power Supply)
ID card door access system
CUTE AREA TECHNICAL
Check-in and passenger manifest system
Baggage and Cargo recognition and classification system
Passenger-luggage matching system
CNS / ATM TECHNICAL
ILS (Instrument landing system)
VOR/DME
PSR/SSR area radars
TDWN
ATC
Radio (Walkie Talkie)
Telephone System
ATC controller desk microphone system
ATC controller screen
ATC VHF frekans

Determination of the Cyber Attack Effect of Airport Systems

- **Likelihood of Occurrence, Discoverability, Severity Scale:** After the existing systems have been removed, it should be asked what happens if each system is out of circuit in the event of a possible cyber-attack. The effect of the deactivated system on the airport needs to be measured. Probability, Discovery, Severity Scale should be used for this. Below is a possibility of Occurrence, Discovery, and Severity Scale for the ID card doorway system which is one of the critical assets for the airport (Table 3).

Table 3 Possibility of Occurrence, Discovery, and Severity Scale for the ID Card Doorway System.

Likelihood of Occurrence
Deactivation of the ID card doorway system never happens.
Deactivation of the ID card doorway system is only possible with internal assistance / tampering.
Deactivation of the ID card door switching system is only possible with more than one software / hardware fault
Deactivation of the ID card doorway system is only possible with a large planned attack / large amount of time and effort and luck
Deactivation of the ID card doorway system is possible with a medium level attack information (a simple Internet search)
Deactivation of the ID card doorway system is possible with a specialized attack information (professional experience and / or training required)

The ID card door access system can be deactivated by an accident caused by personnel and / or an outside party
An accidental attempt by a staff member and / or an outside person rarely causes the ID card door access system to be disabled
An accidental attempt by a staff member and / or an outside person often causes the ID card door access system to be disabled
Disabling the ID card door switch system is a possible accident.
Disabling the ID card door switch system is a situation that can be caused by a planned attack.
Evaluate the possibility of disabling the ID card doorway system

Discoverability
Deactivation of the ID card door access system is instantly discoverable by all employees
Deactivation ID card door access system can be discovered instantly by a single user or several employees
Sudden awareness is not possible if the ID card door access system is disabled
Deactivation of ID card door access system can be discovered before next work / shift
It is not possible to discover even after a lot of work / shift has passed through once the ID card door access system is disabled
Evaluate the discovery of ID card door access disabling

Severity
Deactivation of the ID card doorway system is only an undesirable situation, it does not affect working.
Deactivation of the ID card doorway system affects the effectiveness of working at a serious level but does not affect flight safety
Deactivation of the ID card doorway system disrupts one or more work orders and causes a disaster at the catastrophic level in aviation safety
Evaluate the effect of disabling the ID card door access system

Alternate systems
There are alternative systems to be used if the ID card door access system is disabled
Example from alternative systems / systems
Other things you want to declare

- **Confidentiality, Integrity, Accessibility Scale:** In the event of a possible cyber-attack on airport systems, the confidentiality of the information may be violated. Systems should be questioned for privacy reasons. However, in terms of integrity (unauthorized modification / incorrect replacement) each system should be evaluated. Airport critical systems should be questioned in terms of accessibility / availability. The scale to be used for this is the Scale of Confidentiality, Integrity, Accessibility developed under ISO 27001. The following table has been prepared so that the scale is answered yes / no. Each entity (airport system) can thus be easily assessed by personnel working in the unit concerned. A sample work is given in Figure 3-4-5.

Confidentiality

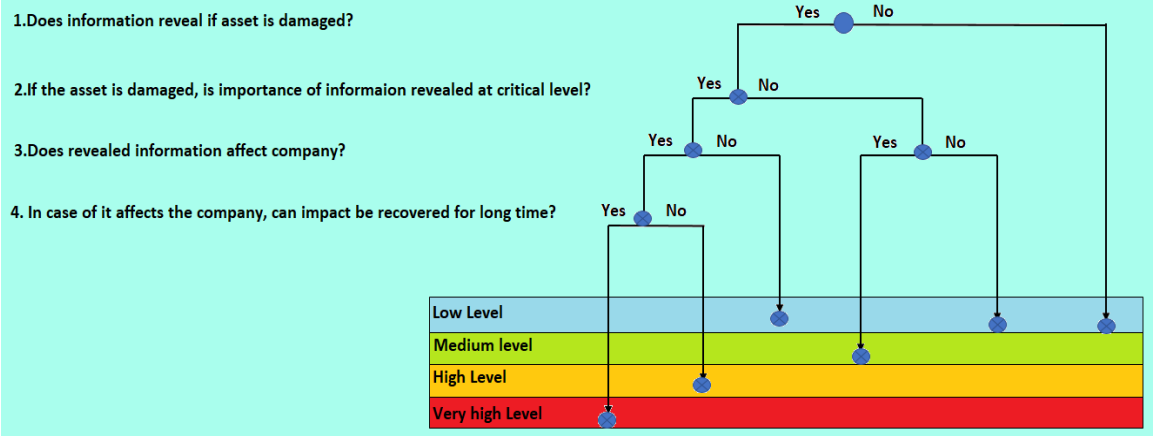


Figure 3 Confidentiality Scale

Integrity

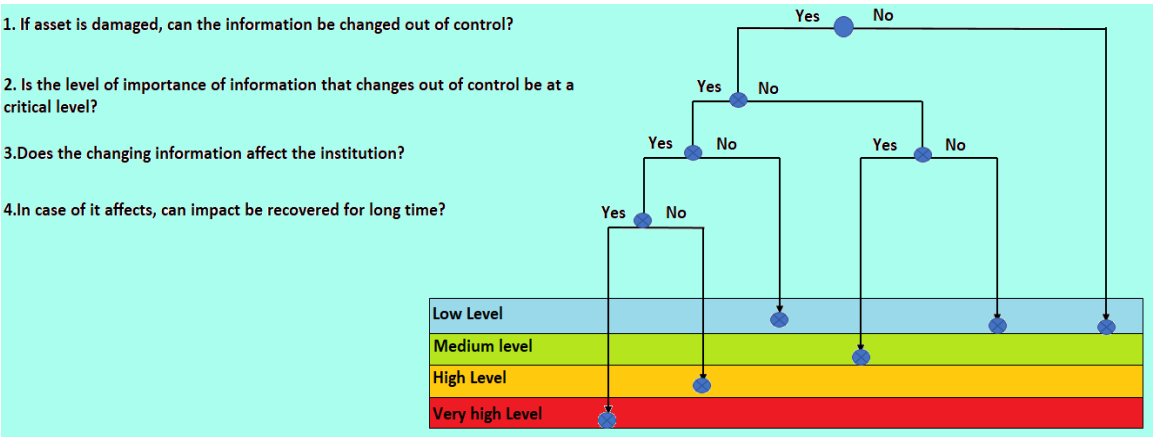


Figure 4 Integrity Scale

Accessibility

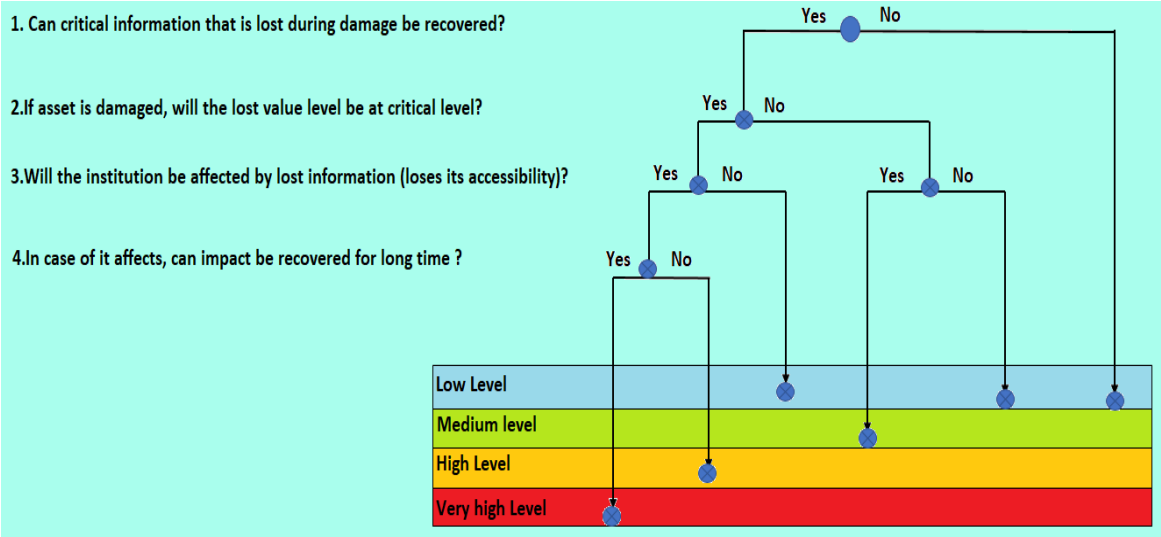


Figure 5 Accessibility Scale

Conclusion and Recommendations

People have felt the need to take measures against the elements that threaten them for years. Security is one of the most basic needs of an individual or an enterprise. Therefore, security is in the class of necessities.

Changing life, technology and society conditions are leading to a shift in security perspective. While the number of electronic-based systems and virtual platforms that people and businesses use has increased, security needs and threats have changed accordingly.

The airports are under the threat of terrorist organizations for economic, socio-cultural and political reasons. Physical security threats have begun to evolve into threats in the virtual platform due to changing ways of doing business.

The main objective is to develop a FEMA scale specific to the intended airports of our research. In the scope of this research, firstly literature search related to cyber security has been done. In the second part of the study, measures taken by the state on cyber threats in public areas such as airports are explained. In the last part, a FEMA scale was developed which consisting three airport-relating steps. It is planned that the scale developed in the survey will be applied at airports. A warning has been received that the sharing of this application by many airports would constitute a significant security breach when scales were sent to airports. Thus, scale experiment could not be realized.

Airports are one of the important sub-structures of aviation that makes hosting more than one systems. For this reason, there are many systems used in airports. The scope of the research is limited only to the systems under control of the airports. The systems used by other airport operators are not included in the survey. For example, the systems that ground services using have been ignored.

In the next research it is aimed to use this scale at an airport and to use it for internal reporting. It is hoped that study will contribute significantly to the safety of cyber security at airports if the research report is supported by internal tests of leaks and DDoS leak.

REFERENCES

Ateş, S. S., & Üzülmez, M. (2016_a). Airport Slot Coordination System: An Implementation at Ataturk Airport. *Global Business Research Congress (Gbrc)*, 99-104, İstanbul: Pressacademia Procedia.

Ateş, S., & Üzülmez, M. (2016_b). System Analysis of Airport Capacity and Slot Coordination at Ataturk Airport. *Research Journal of Business and Management*, 3(3), 248-249.

Aydın, F. (2012). Cyber Security in National Protection of Turkey. Çankaya Üniversitesi Fen Bilimleri Enstitüsü Yayımlanmamış Yüksek Lisans Tezi, Ankara.

Bilgi Teknolojileri ve İletişim Kurumu (2017). USOM ve Kurumsal SOME'ler. Retrieved from btk.gov.tr: https://www.btk.gov.tr/tr-tr/sayfalar/Sg-usom-ve-kurumsal-some, Accessed 12.10.2017.

Center, M. S. (2016). Microsoft Safety & Security Center. Retrieved from Microsoft Corporation: http://www.microsoft.com/Security/Pc-Security/Botnet.aspx, Accessed 26.10.2016.

Cesare, S., & Xiang, Y. (2010). Classification of Malware Using Structured Control Flow. Australasian Symposium on Parallel and Distributed Computing (pp.1-2). Brisbane, Australia: Central Queensland University.

Computerhope.com. (2016). Computerhope. Retrieved from Computerhope.com: http://www.computerhope.com/Jargon/H/Hacker.htm, Accessed 12.10.2016.

Çeliktaş, B. (2016). Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme. Karadeniz Teknik Üniversitesi Sosyal Bilimler Üniversitesi Yayımlanmamış Yüksek Lisans Tezi, Trabzon.

Dijitalx.com. (2017). Siber Olaylarla Mücadele Ekibi Nasıl Eğitiliyor. Retrieved From dijitalx.com: http://www.dijitalx.com/2015/05/14/siber-olaylara-mudahale-ekipleri-nasil-egitiliyor/, Accessed 10.10.2017.

Doğantimur, F. (2009). ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği. Ankara: T.C. Maliye Bakanlığı Strateji Geliştirme Başkanlığı.

E Byres, J. L. (2004). The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems. Proceedings of the VDE Congress (pp. 5-6). Burnaby, Bc, Canada: British Columbia Institute of Technology.

Gandotra, E., Bansal, D., & Sofat, S. (2014). *Malware Analysis and Classification: A Survey*. Journal of Information Security, pp.56-64.

Gocen, U. (2015). Aladin Airports Landside and Air-Land Side Attacks' Detection and Prevention / Full Project Proposal. Eskişehir: Itea 3.

Gramatica, M. D., Fabio Massacci (Member, I., Shim, W., Tedeschi, A., & Williams, J. (2015). It Interdependence and the Economic Fairness of Cyber-Security Regulations for Civil Aviation. United Kingdom: Durham Research Online.

Haberleşme Genel Müdürlüğü (2014). Sektörel Some Kurulum ve Yönetim. Ankara: T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı.

Havacılık Güvenliği Daire Başkanlığı (2016). Genelge Hgd – 2015/1. Konu : Kurumsal Siber Olaylara Müdahale Merkezi. Ankara: Sivil Havacılık Genel Müdürlüğü.

Herdem, A. Ş. (2017). Siber Saldırılar Havacılığı Tehdit Ediyor. Retrieved From Airporthaber: http://www.airporthaber.com/havacilik-haberleri/siber-saldirilar-havaciligi-tehdit-ediyor.html, Accessed 07.09.2017.

Islam, R., Tian, R., Batten, L., & Versteeg, S. (2010). Classification of Malware Based on String and Function Feature Selection. Second Cybercrime and Trustworthy Computing Workshop (pp. 9-11). Melbourne: Deakin University.

Jinsoo Shin, H. S. (2016). Cyber Security Risk Evaluation of A Nuclear I&C System Using Bayesian Networks and Event Trees. Gyeonggi-Do, Republic of Korea: Kyung Hee University.

Koç, F. (2008). BGYS-Varlık Envanteri Oluşturma ve Sınıflandırma Kılavuzu. Kocaeli: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü.

Lee H.L., Liu Y.T., Chen, S.C., Tang, S.K., Huang, C.P., Huang, C.H., Chang, Y.L. Chang, K.W. & Chen, K.Y. (2002). A Comparative Study of Protocol Analysis for Spatiality of A Text-Based Cyberspace pp. 262-266, Hsinchu,Taiwan: Graduate Institute of Architecture, National Chiao Tung University.

Lord, N. (2012). Common Malware Types: Cybersecurity 101. Retrieved from Veracode: https://www.veracode.com/Blog/2012/10/Common-Malware-Types-Cybersecurity-101, Accessed 15.10.2017.

Ulusal Siber Olaylarla Müdahale Merkezi (2017). USOM Hakkında. Retrieved from usom.gov.tr: https://www.usom.gov.tr/Hakkimizda.html

Miller, S., Wagner, C., Aickelin, U., & Garibaldi, J. M. (2016). Modelling Cyber-Security Experts' Decision Making Processes Using Aggregation Operators. Computer & Security, 62, 229-232.

Normatürk. (2017). Siber Olaylara Müdahale Ekibi (SOME). Retrieved from Normatürk: http://normaturk.com/some/, Accessed 14.09.2017.

Oxforddictionaries (2016). Retrieved from Oxforddictionaries: https://en.oxforddictionaries.com/definition/Us/Cyberspace, Accessed 11.11.2017.

Park, Y., Reeves, D., Mulukutla, V., & Sundaravel, B. (2010). Fast Malware Classification by Automated Behavioral Graph Matching. Raleigh, Nc: Department o Computer Science Department.

SHGM (Sivil Havacılık Genel Müdürlüğü) (2014). Kurumsal Some Kurulum ve Yönetim Rehberi. Ankara: T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı.

Taş, Y., & Koç, K. H. (2017). Hata Türü ve Etkileri Analizi (FMEA) Tekniğinin Mobilya Endüstrisine Yönelik Uygulaması. Retrieved from aydin.edu.tr: http://iaud.aydin.edu.tr/makaleler/yil2sayi5/iaud_yil_2_sayi_5_makale_9.pdf, Accessed 09.10.2017.

TechTarget (2016). Retrieved from Techtarget: http://searchsoa.techtarget.com/definition/cyberspace, Accessed 12.09.2017.

Tosun, A. (2016). A Survey about the Integration of Social Engineering Attacks with Cyber Security Exploiting Turkish Vulnerabilities in Turkey. Middle East Technical University The Department of Information Systems Master Degree' Thesis, Ankara.

Ulusal Siber Olaylara Müdahale Merkezi (2017). Retrieved from Wikipedi: https://tr.wikipedia.org/wiki/ulusal_siber_olaylara_m%c3%bcdahale_merkezi, Accessed 10.09.2017.

Wert, M. (2016). Study.com. Retrieved from study.com: http://study.com/academy/lesson/cyber-threats-definition-types.html, Accessed 18.10.2017.

Willson, D. (2016). Chapter 3 – Who are the Hackers? Cyber Security Awareness for Ceos and Management, 25-29.

Yagoda, B. (2014). A Short History of "Hack". Retrieved from The New Yorker: http://www.newyorker.com/tech/elements/a-short-history-of-hack, Accessed 09.09.2017.