УДК 005.922.1:658.11(497.7)

MODERN COMPANIES THROUGH THE PRISM OF A MODERN SECURITY CONCEPT

Gjorgji Alceski[1]
TAV Macedonia Airport St. Paul the Apostle Ohrid

Tomislav Tuntev[2]
Civil Aviation Agency of the Republic of Macedonia

Abstract: In today's conditions of rapid technological progress and the increasingly emphasized need to monitor modern business, it becomes practically unimaginable without an adequate security concept, which will guarantee dealing with a large number of threats, risks and dangers. Threats aimed at companies and especially those that belong to the group of critical infrastructures as one of the most dangerous threats, but also the large number of security threats caused by social deviations, pandemics, natural disasters, technical-technological breakdowns, human errors, technical deficiencies, not the appropriate education etc. they are also slowly changing the concepts of company security. On the other hand, if we take into account the complexity and dynamic development of the information sector, which is so complex from the point of view of identifying threats and weaknesses. Hence, the strategy of every serious company in the security segment should be built on the basis of the basic principles for dealing with threats, dangers and risks, which implies a wider obligation, first of all, of the management, but also of all stakeholders in the security system. It represents a complex structure of mutual relations and processes that penetrates into the sphere of multidisciplinary application of a large number of experts.

Following business interests on the one hand and the possible direct negative impact on security on the other, which can lead to a fatal outcome on the profitability and sustainability of the company's core business but also on the wider social interest, undoubtedly requires a systematic approach by all management levels. At the same time, it represents a permanent upgrade of work programs and procedures, the role of company intelligence, the development and application of advanced security equipment for protection, etc. Therefore, security departments and educated personnel need to be focused on multiple fields of the security system. Following the positive practices of a large number of successful companies, this paper will present models for improving the security of the protected object through the implementation of several aspects: regulatory, organizational, structural, technical, etc., with a tendency to offer certain solutions and practical solutions that would improve and advance the existing security system of a modern company.

Keywords: company security, security management, coordination, protective systems

[1] Contact address: Gjorgji.Alcheski@tav.aero

[2] Contact address: tomislav.tuntev@tav.aero

Introduction

Every modern company strives for its own development, which includes top planning, identifying threats, risks and dangers of any type and character, as well as dealing with them in the direction of achieving its goals and strategies for the company's growth. There is no doubt that managers and companies that use proven management techniques and practices in their decision-making and actions further increase efficiency. However, with the increase in productivity, development, the performance of the company grows proportionally and the security challenges that must be treated as a strategic interest of the company. Therefore, security must be one of the priorities of all modern companies, and the way of organization will depend on the assessment of the functionality of the system. Can't load full resultsTry again

Retrying...

Retrying...

Thus, security becomes a business function that aims to protect the company from external, internal or combined harmful influences. In a broader systemic sense, company security unites several functional entities such as economic security, information security, social security, legal security and other areas of security (Keković 2018). Any neglect of security in companies leads to serious losses, failure and serious consequences.

Designing a company's security system represents a long-term activity that consists of several characters, from the initial basis and answer to the question of what it is that we are protecting, further, what are the threats, risks and dangers, their type and character, and up to the implementation of the security concept. Given the latest developments related to the coronavirus pandemic that has caused a global health and economic crisis, as well as the Russian attack on Ukraine this year, we are entering new economic, health, social and security challenges that we must face and apply all latest crisis management modalities because the probability of the crisis being limited to only one country or region is practically impossible. It is necessary to take into account several scenarios for the escalation of the crisis, but also the triggering of new crises as a result of the conflict. For those reasons, every large company that has a strategic interest of the state or is declared as a critical infrastructure needs to develop management plans in crisis and post-crisis recovery.

However, in order to cope with the complexity in the implementation of a modern security concept of a company, first of all, a systematic study of all the company's activities is needed, definition of the level of protection, responsibilities and competences of all actors, processing of the information obtained by the method of company intelligence, strategic determinations, eventual dependence and all threats arising from economic, social, social and other types of character, all supported by a scientific and professional approach.

Bearing in mind the terminological distinction around the term security, which for the purposes of this paper will unite the terms safety and security, where in some companies these are different areas of action and protection - mostly in large corporations, but very companies that unite these activities within one sector or field of action are often found. Hence the complexity of company security and the security concept itself.

1. Contemporary corporate challenges

Each company has its own value, unique characteristics, social significance, diversity of the workforce, innovation, various risks, threats, dangers, difficulties in the realization of the work process, but also in the implementation of security measures. A large number of companies are so complex in the area of security that they require highly professional support from a large number of experts from different fields, therefore making this approach to security multidisciplinary. At the same time, there is a full understanding that threats to the security of the company cannot be the full responsibility of the company itself, but usually represents a broader obligation of several security entities and structures in the state. This comes to the fore especially when dealing with a company of national interest or the so-called "critical infrastructures".

Basically, managers at all levels and in all departments, whether it is for small, medium or large companies, further for-profit or non-profit organizations, are mostly used with the four essential managerial tasks: planning, organizing, leading and controlling and all in the direction of creating a highly functional organization. But it should be emphasized that, in today's world, managers face at least five more major challenges such as: building a competitive advantage, maintaining ethical standards, managing a diverse workforce, using new information systems and technologies, and practicing global crisis management.[3]Given that security has serious impacts in all of the preceding challenges, forms of action emerge to reduce or eliminate harmful impacts.

In addition to the forms of building a competitive advantage, which include superior efficiency, quality, speed and flexibility, as well as innovation and responsibility towards customers, we would also mention information as a resource in building a competitive advantage, which enters the domain of company security. The collection of information, but also the protection against "leaking" of confidential information is becoming a dominant activity of the security services of every major company. Legal collection of business information and its adequate analysis that supports management in making appropriate decisions or building future development strategies in many companies is of top priority. There are a number of techniques and methodologies for collecting information, but the most important thing is to emphasize that it is necessary to apply the methodologies for collecting information that belong to the so-called "white zone", which is characterized by the application of legal and ethically permitted methods. The business intelligence function represents the corporation's ability to understand the market environment and effectively adapt to all changes in the environment, that is, to compete with competitors in a way to be more successful. In that sense, Business Intelligence is knowledge that exists with the current trends of the company level to analyze future state of the business environment, it is also an organizational instrument for gathering,[4]In addition, this direction also includes the process of protecting the company from the illegal collection of information, i.e. dealing with

[3] Gareth R. Jones (Texas A&M University), Jennifer M. George (Rice University) McGrew/Irwin 2008 - Contemporary Management ISBN 978-608-4522-00-3 str 27.

[4] Trivan D. Meaning in words - notification actions for corporate and national security - Corporate security Chrestomatija Z. Kekovic, I. Dimitrijevic, N. Šekarić University of Belgrade - Faculty of Security - Belgrade 2018.

the methods of so-called industrial espionage, which belong to the group of acts that are not in accordance with ethical norms or completely belong to the illegal actions.

The next challenge that many companies face is the correct selection of personnel and the ethical standards that need to be met. From the aspect of security as an integral part of business management, it is necessary to make precise criteria commensurate with specific needs and tasks. A company employing personnel must ensure that these individuals meet the standards and possess the necessary competencies to perform assigned functions at an acceptable level. Also "competence" means being able to demonstrate appropriate knowledge and skills. Competencies acquired by individuals prior to recruitment may be taken into account when assessing training needs, but one of the most important criteria is a clean background check. This primarily means determining the identity of the person on the basis of an evidentiary document and criminal records in all states of residence during at least 5 previous years. Every new employee needs to be subjected to security checks, and such checks must be repeated at a certain period of time. The security checks of the persons who work or are employed in the company, and especially in a company that represents or is part of the national critical infrastructures, should include checks on the identity and previous past of the person in terms of any criminal past and eligibility for his employment.

Managing a diverse workforce today represents a challenge for every modern company. Highly trained and motivated staff is one of the keys to success. Big and strong corporations place great emphasis on educations that are basically based on a combination of knowledge, skills, abilities, behaviors, etc. The purpose of this approach is connected with the need for successful completion of the work and through that realization of the strategic interest of the company, maintenance or cultivation of knowledge, application of acquired competences in the work environment and the ability to transfer competences. In this context, it is necessary to mention the need for both short-term trainings, solving current trainings, and the serious need for development trainings or strategic long-term educations. As one of the main strategic management, it also implies the attraction or recruitment of the necessary staff, above all the so-called "talents", who in the future, through appropriate education and career development, will represent the basis of the companies. In the context of a lack of quality personnel, one of the challenges is strategies for attracting employees for future roles and positions. Providing training and development to current employees is a popular strategy used by most organizations to retain quality staff.[5]However, it can be safely said that security awareness is one of the most important factors for overall security, with the ultimate goal of preserving human lives and material goods.

In order to achieve an adequate security policy of the company, every single employee, regardless of the job position and professional profile, needs to have elementary knowledge of security, especially for the duration of his work duties. The worker is required to be careful and inform about any suspicious or abnormal situation. Safety awareness also implies compliance with the safety regulations that apply to all employees in the company, but it also implies reacting in certain specific situations where you need to show determination, how to solve a certain situation correctly, whether in normal conditions or in emergency situations.

[5] Seven Trends in Corporate Training and Development - Dr. Ibraiz Tarique.https://drive.google.com/file/d/1uJJ68SO9kYRxRMN4swssQIQoBvdn738F/view

So safety is everyone's responsibility! "Promoting an effective safety culture is critical to achieving good results."[6]

Safety culture is a set of norms, beliefs, values, attitudes and assumptions that are inherent in the daily operation of an organization and are reflected by the actions and behavior of all entities and personnel within the organization.

Using new ***information systems and technologies in modern business*** is the most dominant challenge that enables a wide range of benefits and the development of new opportunities and innovations. However, the complexity and dynamic development of the sector makes it so complex in terms of identifying threats and weaknesses that it requires enormous company cooperation and a creative way of protection. Although the infrastructure related to information technology has a certain level of inherent elasticity, due to the large interdependencies it represents a challenge especially in criminal actions aimed at companies. Dealing with this kind of threats is a very complicated task, because cyberspace itself is a very large and uncertain area that is difficult to delineate and define, so that computer systems are a constant target of attacks. Global networking in the system of communication and information technology has become the basis of the functioning of organized crime, while terrorism has received another tool in its hands. An attack on information systems can be defined as a direct action against a network or an information system, with the aim of unauthorized interception or termination of an operation, taking control or destroying, changing or corrupting data (with memorization or processing).[7]

Information society is basically based on knowledge and innovation, so that a large number of citizens through electronic communication infrastructures and digital technologies have easy and cheap access to information and knowledge. But in addition to the positive side, we also need to face the negative consequences of technology.[8] For those reasons, the security of this sector needs to be based on: protection of information systems and networks, instrumentation, automation and control systems, internet, provision of fixed telecommunications, provision of mobile telecommunications, radio communication and navigation, satellite communication, broadcasting etc.

From the perspective of global crisis management, it is a fact that today managers are facing one of the biggest tests in the past few decades. Considered from several aspects, the modern manager needs to place the emphasis on a global aspect in order to provide appropriate solutions to the current geopolitical situations. We are witnessing the coronavirus pandemic which resulted in a global economic crisis, primarily due to the introduction of a ban on movement and the closing of borders and a decline in economic activity, while the adoption of a series of health and economic measures aimed at the population and businesses resulted in a significant deterioration of the fiscal and balance sheet positions of countries. In this context, as the most current event, it is necessary to mention the Russian attack on Ukraine this year and the entry into new global problems that will directly or indirectly affect the companies. Finding ways to deal with the crisis is one of the priorities of all managers.

[6] https://www.icao.int/Security/Security-Culture/Pages/default.aspx

[7] Stallings William, Network and Internetwork Security – Principles and practices, Prentice Hall, Englewood Colleges, New Jersey 1995., pp 29 – 30 / Taken from Bakreski O. Trivan D. Mitevski S. Skopje 2012 – Corporate security system p.243

[8] https://www.dhs.gov/information-technology-sector, Retrieved 10/24/2015year

2. Current events and their impact

The COVID-19 pandemic has deeply affected the operation of all activities of social life. The global impact of COVID-19 on aviation, tourism, trade and the economy in 2020 was:

- **Air passenger traffic:**An overall reduction of air passengers (both international and domestic) ranging from 60% in 2020 compared to 2019 (by ICAO)
- **Airports**: An estimated loss of approximately 64.6% of passenger traffic and 66.3% or over USD 125 billion airport revenues in 2020 compared to business as usual (by ACI)
- **Airlines**: A 65.9% decline of revenue passenger kilometers (RPKs, both international and domestic) in 2020 compared to 2019 (by IATA)
- **Tourism**: A decline in international tourism receipts of USD 1.3 trillion in 2020, compared to the USD 1.5 trillion generated in 2019 (by UNWTO)
- **Trade**: A fall of global merchandise trade volume by 5.3% in 2020 compared to 2019 (by WTO)
- **Global economy**: An estimated -3.3% to -4.3% contraction in world GDP in 2020, far worse than during the 2008–09 financial crisis (by IMF and World Bank)[9]

The pandemic crisis caused by covid 19 through the lens of the airline industry looks like this:

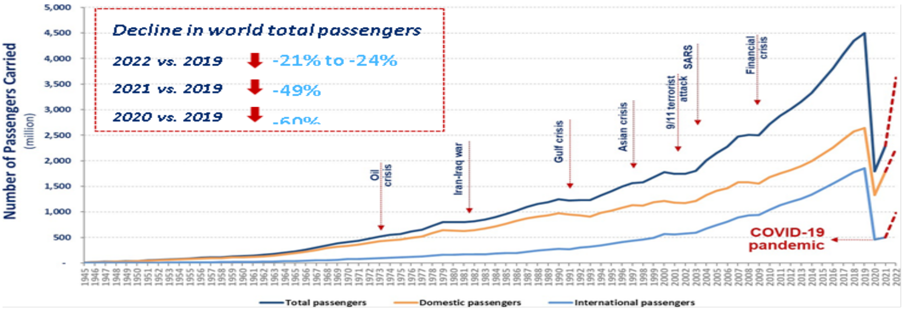
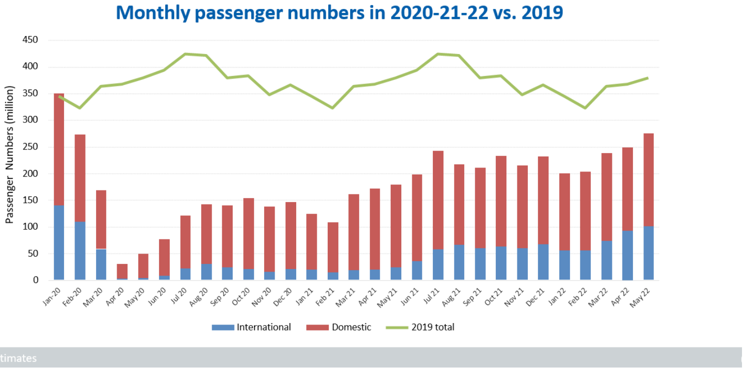


Table No. 1. *World passenger traffic evolution - 1945 – 2022*[10]


Monthly passenger numbers in 2020-21-22 vs. 2019

Source: ICAO estimates

Table No. 2. *Monthly passenger numbers in 2020-21-22 vs. 2019*[11]

[9] www.icao.int/sustainability/Documents/COVID-19/ICAO_Coronavirus_Econ_Impact.pdf-Author/analysis by: Toru Hasegawa; Data compilation by: Sijia Chen; ADS-B data retrieval by: Lan Duong

[10] https://www.icao.int/sustainability/Documents/COVID-19/ICAO_Coronavirus_Econ_Impact.pdf

[11] Effects of Novel Coronavirus (COVID-19) on Civil Aviation: Economic Impact Analysis Montréal, Can-

The COVID-19 impact on world scheduled passenger traffic for year 2020 (actual results), compared to 2019 levels:

- Overall reduction of 50% of seats offered by airlines
- Overall reduction of 2,703 million passengers (-60%)
- Approx. USD 372 billion loss of gross passenger operating revenues of airlines

The COVID-19 impact on world scheduled passenger traffic for year 2021 (preliminary estimates), compared to 2019 levels:

- Overall reduction of 40% of seats offered by airlines
- Overall reduction of 2,201 million passengers (-49%)
- Approx. USD 324 billion loss of gross passenger operating revenues of airlines

The COVID-19 impact on world scheduled passenger traffic for year 2022 (estimated results), compared to 2019 levels:

- Overall reduction of 15% to 18% of seats offered by airlines
- Overall reduction of 921 to 1,079 million passengers (-21% to -24%)
- Approx. USD 133 to 155 billion loss of gross passenger operating revenues of airlines

International passenger traffic (2022, vs. 2019)

- Overall reduction of 20% to 25% of seats offered by airlines
- Overall reduction of 457 to 544 million passengers (-25% to -29%)
- Approx. USD 96 to 112 billion loss of gross operating revenues of airlines

Domestic passenger traffic (2022, vs. 2019)

- Overall reduction of 12% to 14% of seats offered by airlines
- Overall reduction of 464 to 537 million passengers (-18% to -20%)
- Approx. USD 37 to 43 billion loss of gross operating revenues of airlines[12]

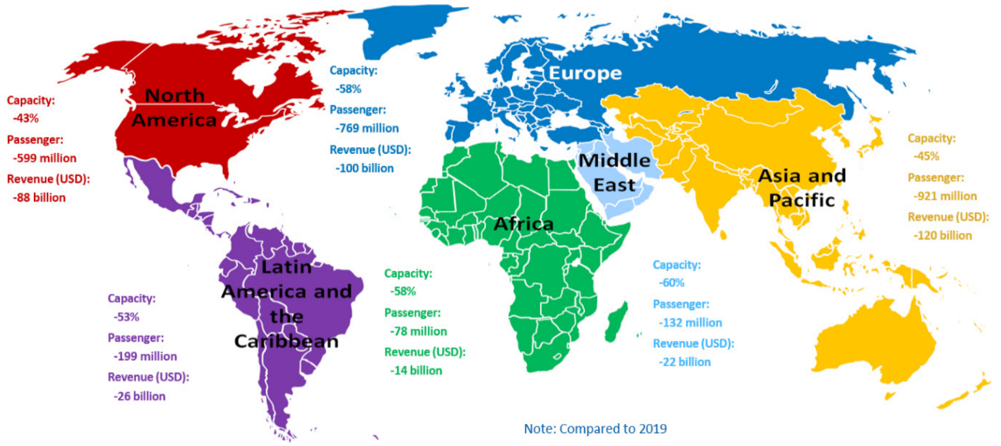


Table No. 3. *Estimated impact on passenger traffic and revenues by region for 202013*

ada 15 June 2021 Economic Development – Air Transport Bureauh ttps://www.icao.int/sustainability/Documents/COVID-19/ICAO_Coronavirus_Econ_Impact.pdf

[12] https://www.icao.int/sustainability/Documents/COVID-19/ICAO_Coronavirus_Econ_Impact.pdf

[13] https://www.icao.int/sustainability/Documents/COVID-19/ICAO_Coronavirus_Econ_Impact.pdf

The actual impacts will depend on the duration and magnitude of the outbreak and containment measures, the degree of consumer confidence for air travel, and economic conditions, etc.

If we consider that the global economy has not yet recovered from this shock, the Russian attack on Ukraine took place on February 24, 2022, which worsens the prospects for further recovery.

It is imperative for countries, industries and all stakeholders to have reliable information and a tool to monitor and assess the impact of COVID-19 and other adverse situations to use key indicators to make decisions based on relevant indicators.

We must be sure that due to current developments, countries with direct trade, tourism and financial exposure will feel additional problems in the future. Economies dependent on oil imports will see wider fiscal and trade deficits and greater inflationary pressure, although some exporters such as those in the Middle East and Africa may benefit from higher prices, but basically the problem in this field will remain current. Also increases in food and fuel prices may encourage a greater risk of unrest in some regions, posing a serious security risk. In the longer term, war could fundamentally change the global economic and geopolitical order if energy trade is altered, supply chains are reconfigured, payment networks are destroyed and countries reconsider the possession of reserve currency, difficulties with the trade of technology, etc. These effects will fuel inflation and slow the recovery from the pandemic. Eastern Europe would be affected by increased financial costs and an increase in refugees. It has absorbed most of the three million people who have recently fled Ukraine, according to United Nations data. European governments may also face fiscal pressures from additional spending on energy security and defense budgets.[14]Given the fact that many companies openly support Ukraine and cut off trade and investment in Russia, it increases the possibility of becoming a target of cyber and other types of attacks.

So, the Ukrainian crisis represents a continuation of the crises in the twenty-first century and represents the beginning, not the end, of the more acute phase of the crises that follows today. Deep analyzes made by a huge number of experts, including the scientific community, provide guidelines that fall into the category of national security from several aspects.

3. Development of plans for work in emergency circumstances

The COVID-19 pandemic has shown many companies the importance of establishing comprehensive contingency plans for an unplanned event, while the Ukrainian crisis only proves the necessity of such an approach. The fact is that companies with adequate plans were able to react more quickly when the pandemic caused by COVID-19 began to escalate and the losses or damages were kept at an acceptable level compared to companies that entered the pandemic unprepared and needed time to adapt to the new situation.. This meant that many businesses were woefully unprepared and forced business leaders to refocus their approach to risk management.

Today's challenges, of course, require a complex multidisciplinary approach in solving, that is, managing companies, especially companies that belong to vital facilities for

[14] IMF (International Monetary Fund) https://blogs.imf.org/2022/03/15/how-war-in-ukraine-is-reverberating-across-worlds-regions/

national security and the well-being of citizens, and establishing a delicate balance between maintaining working condition and supporting economic recovery from newly emerging situations. Therefore, potential risks need to be identified before they become real problems.

The strategy of any serious company, and especially one with a critical infrastructure in the security segment, should be built on the basis of the basic principles of security risk management, which implies a multifaceted approach to mitigating threats. According to the definition given for risk analysis by the European Commission in Directive 114 from 2008, it is presented as a review of appropriate hazard scenarios that would assess weaknesses and potential negative impact on the operation or destruction of critical infrastructure.[15]

In the green book of the European Commission, related to the protection of critical infrastructure, the term risk is presented as: the possibility of loss, damage or injury. While the level of risk is a state of two factors:

- the value of the owner/operator's assets and the impact of loss or alteration of the property, and
- the likelihood that a specific vulnerability will be exploited for a specific threat[16]

In the same document, the term threat is defined as: any indication, situation or event, with the potential to disrupt or destroy critical infrastructure, or any element thereof. The overall approach to hazards includes, accidents, natural disasters as well as deliberate attack. It can also be defined as the intention and ability to take actions that will be detrimental to the property. The term vulnerability represents: a characteristic of an element or operation that makes it susceptible to destruction or incapacitation by a certain threat to the critical infrastructure.

If we look at the risks through the companies that are determined as critical infrastructures, we will see that it is not possible to eliminate all risks, but they require the design of a rational decision-making process. With efficient management and allocation of protective resources in combination with available security technologies - risks can be controlled and the danger satisfactorily mitigated, that is, brought to an acceptable level. The risks faced by companies are versatile and can be grouped into several categories such as: financial, operational, strategic, security, etc. In this context, businesses must once again expand their competencies to balance short-term and long-term challenges and measures.

That is why there is a need to develop a greater number of scenarios and to develop contingency plans that develop more measures and activities, including the security impacts on companies. As the overall severity and duration of the COVID-19 pandemic and the Ukraine crisis are still uncertain, indicative scenarios need to be developed to help gauge the potential economic and security implications.

Such company plans will be submitted to the line ministries as well as the state body in charge of managing the crisis caused by the current global developments. Among other things, the plans could elaborate on alternative sources of supply, redefining production strategies, analysis of inventory and timely replenishment, investment in artificial intelligence, elimination of interdependencies, security implications, etc.

[15] COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008

[16] GREEN PAPER ON A EUROPEAN PROGRAM FOR CRITICAL INFRASTRUCTURE PROTECTION Brussels, 17.11.2005 COM (2005) 576 final

A contingency plan is a roadmap of action designed to help a company respond effectively to a significant future incident, event, or situation that may or may not occur. A contingency plan is sometimes called a "Plan B" or back-up plan because it can also be used as an alternative course of action if the expected results are not achieved.

The plans that are made in modern companies represent strategic documents that should provide an answer to many situations that can disrupt operations beyond the planned plan. These plans, among other things, can prevent risks but also respond post-crisis for faster recovery. In general, all major companies develop plans for unforeseen situations based on natural disasters, fires, accidents, etc. or generally dangerous acts of illegal behavior on a larger scale in which state bodies also play a role, but today's developments give an objective reason for expanding such plans by analyzing a wider geopolitical dimension.

From the point of view of aviation as a very sensitive industry we can say that it has a very careful approach to making precise planned operations because any direct or indirect disturbance can have significant and far-reaching negative impacts. Such disruptions may result from aircraft, airport and air navigation emergencies, natural disasters or other causes, including public health crises, and the impacts include significant financial, environmental, social and/or material damage, which may have a spillover effect on interrelated industries such as tourism and trade. These plans are used to identify potential risks facing the company; determine how those risks will affect business operations; implement controls and measures designed to mitigate those risks; of course as well as monitoring, testing and evaluating the strategic plan to keep it current.

The International Civil Aviation Organization (ICAO), in its capacity to develop standards and recommended practices (SARPs) for the safety, efficiency and regularity of international civil aviation, publishes specific SARPs to address the necessity and importance of emergency response planning and coordination for various stakeholders of the aviation system. Other international organisations, including the Airports Council International (ACI), the International Air Transport Association (IATA) and the Civil Air Navigation Organization (CANSO), have also published documents and manuals with guidance and best practices to support their respective stakeholders. in establishing emergency response and contingency plans.

Unfortunately, after the crisis recovery from the Pandemic caused by KOVID 19 in the part of the airline business, it did not give the desired results, especially in the part of human resources management. They need to rethink their strategy in terms of flexibility and creativity to anticipate and cope with staff shortages. Even though the plans elaborate the specific roles, set of activities and time frames for responding to unexpected situations, obstacles or potential disruptions, the omissions made in the part of planning for post-crisis recovery or the return to so-called normal conditions are followed by very serious consequences. . As a result of inactive implementation of plans or insufficient planning analysis, coordination and training, a large number of canceled or delayed flights occurred.

International organizations are therefore encouraging countries and operators to have business continuity plans that go beyond immediate mitigation plans for unplanned incidents. The goal is to build and improve organizational resilience and the ability to quickly and effectively recover from any local, regional or global disruption. It is necessary to develop several scenarios for the escalation of emergency situations as well as the triggering of new crises as a result of current developments. For those reasons, every large company that has a strategic interest of the state or is declared as a critical infrastructure needs to develop management plans in crisis and post-crisis recovery.

Conclusion

Analyzing the applied practices of large and strong companies, the need for more extensive elaboration and application of modern management, which carries with it the challenges of today, is unequivocally imposed. Any neglect of security in companies leads to serious losses, failure and serious consequences. Designing a company's security system represents a long-term activity that consists of several characters, from the initial basis and answer to the question of what it is that we are protecting, further, what are the threats, risks and dangers, their type and character, and up to the implementation of the security concept. Modern companies considered through the prism of security represent a complex and interdependent set of measures, plans, activities and programs and require the extension of the previous practices. In that direction, the need to implement a framework on which future development strategies should be based in terms of dealing with crises and post-crisis recovery is unequivocally imposed. Therefore, first of all, an institutional approach is needed, a strategic framework is needed in terms of definition, and analogously, a more acceptable methodology is needed to reduce the risks of negative consequences, which is a condition for a stable society, and the reliable performance of the company's strategic functions. Very important is to *invest in personnel in crisis situations is one of the measures for post-crisis recovery.*

The management of companies, especially those declared as critical infrastructures, must be an integral part of all development state programs, especially in the area of safety and prevention of risks, accidents and disasters, and must be integrated into all relevant documents. of the state. Today's developments have confirmed that the seriousness of threats to critical infrastructures and the general impression of responsibility for the protection of national critical infrastructures, which mostly falls on operators, is becoming a state problem.

The new types of threats require, first of all, the organization of the top management continuously 24 hours a day with the involvement of the entire state apparatus. The analysis shows that the coordination between the relevant entities enables a more efficient realization of security goals, as well as reducing risks and dealing with unforeseen situations. Cooperation with state institutions should be aimed at intensifying taking steps to strengthen partnership relations, both in terms of increasing economic and security potential, further defining competencies and a joint position of action and establishing a proactive approach to issues related to crisis situations.

Following the example of aviation, as one of the more regulated areas, the applicability of certain methods, techniques and equipment in other critical infrastructures that are not and/or insufficiently regulated can help in today's conditions. The professional, professional and permanent management of development company policies, which includes a wide range of measures, procedures and procedures in the field of preventive security, but also in the field of dealing with crisis situations and recovery, requires constant development.

The essential characteristic of the risks and the sources of threat are increasingly becoming unpredictable, asymmetric and have a transnational character. Hence, the need for the introduction of assessments, as well as the implementation of methodologies through models adjusted and adapted for specific companies, inevitably arose.

References

- Gareth R. Jones (Texas A&M University), Jennifer M. George (Rice University) McGrew/Irwin 2008 - Contemporary Management ISBN 978-608-4522-00-3.
- COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008
- GREEN PAPER ON A EUROPEAN PROGRAM FOR CRITICAL INFRASTRUCTURE
- PROTECTION Brussels, 17.11.2005 COM(2005) 576 final
- Stallings William, Network and Internetwork Security – Principles and practices, Prentice Hall, Englewood Colleges, New Jersey 1995d.
- Bakreski O. Trivan D. Mitevski S. Skopje 2012 – Corporate security system
- Z. Cakesq, I. Dimitrijevic, N. Šekarić - Corporate Security Curriculum Vitae University of Belgrade - Faculty of Security - Belgrade 2018.
- G. Alceski, T. Tuntev Airports as critical infrastructure - Ohrid 2021.
- https://www.iata.org/en/publications/store/emergency-response-handbook/
- https://www.icao.int/sustainability/ERP/Pages/industry-erpguidance.aspx
- https://drive.google.com/file/d/1uJJ68SO9kYRxRMN4swssQlQoBvdn738F/view
- https://store.aci.aero/product/emergency-preparedness-and-contingency-planning-handbook-first-edition-2014/
- https://blogs.imf.org/2022/03/15/how-war-in-ukraine-is-reverberating-across-worlds-regions/
- https://www.icao.int/sustainability/Documents/COVID-19/ICAO_Coronavirus_Econ_Impact.pdf
- https://www.icao.int/sustainability/Documents/COVID-19/ICAO_Coronavirus_Econ_Impact.pdf
- https://www.dhs.gov/information-technology-sector, Retrieved 10/24/2015.
- https://www.icao.int/Security/Security-Culture/Pages/default.aspx
- https://www.zurich.com/en/knowledge/topics/global-risks/four-ways-conflict-in-ukraine-will-change-approach-to-risk-management