Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4, 3123-3134
2025
Publisher: Learning Gate
DOI: 10.55214/25768484.v9i4.6743

Cybersecurity and its impact on risk management facing tourism organizations – A case study at Baghdad international airport

Muhammad Abd Maktouf[1*], Muthanna Alobaidi[2]
[1,2]Al-Mustansiriya University, College of Tourism Sciences, Iraq; mohammed.abid1989@uomustansiriyah.edu.iq (M.A.M.) muthanna.alobaidi@uomustansiriyah.edu.iq (M.A.).

Abstract: The research aimed to test the impact of Cybersecurity and its dimensions (Political, Economic, Information Protection, Legal, Military, Academic, Educational) in improving Risk Management among Baghdad airport managers. The total community size was 87, and the random research sample was selected using the model (D. MORGIN). A total of 71 questionnaires were distributed, and according to the results, 67 questionnaires were retrieved, all of which were valid for statistical analysis. The program (SPSS v.28) was used to analyze the answers of the sample members. The data were collected, analyzed, and the validity and stability of the study tool were confirmed using parametric statistical methods (Alpha Cronbach) to determine internal consistency for all elements. Percentage and frequency tables were created using the answers of study sample members regarding personal information such as gender, age, educational qualification, and number of years of service. Correlation and regression, mean and standard deviation, and the (T) test for the difference between variables (Independent Sample T Test) were used with Pearson techniques for statistical analysis of data at the level of significance $\partial \leq 0.5$. The results indicated that the availability of cybersecurity and its dimensions was high, while risk management and its dimensions were available moderately. Additionally, the impact of cybersecurity and its dimensions on risk management was noted.

Keywords: *Baghdad international airport, Cybersecurity, Information protection, Risk management.*

1. Introduction

Methodology: Cybersecurity and Risk Management are related and complementary concepts, as cybersecurity represents a set of procedures and policies aimed at protecting information and systems from electronic threats, while risk management embodies the process of identifying, evaluating and implementing the necessary procedures to reduce or avoid Modern Airports have used cybersecurity to face various expected risks that threaten the security of information and navigational systems in which global airports operate, and cybersecurity contributes to its ability to assess risks and determine their level, as well as implement the necessary measures to reduce, reduce and avoid them as much as possible, as well as monitor and evaluate the procedures implemented by its administration, which contributed to improving information security, and airports' compliance with international laws and regulations related to airport safety and security, to be the goal that unites them. Obtaining the confidence of passengers, airlines and their suppliers, so it required the presence and attraction of more technical expertise as a result of the complexity in systems and software, as well as the need for high costs, long time, specialized teams and effective communication with various actors in the success of airports in their risk management.

Importance of Research: The importance of its ability to achieve following.

1. Importance of tourism sector benefiting from the research, as Baghdad Airport is one of the sovereign ports in Iraq, and receives the attention of the state primarily on other sectors, which

History: Received: 7 February 2025; Revised: 11 April 2025; Accepted: 15 April 2025; Published: 30 April 2025
* Correspondence: mohammed.abid1989@uomustansiriyah.edu.iq

prompted the researcher to collect two important variables, cybersecurity and risk management in a model tested for the first time in Iraqi airports.

2. Importance of Study: There are few theoretical studies in a field of Cybersecurity in Tourism sector and therefore there is a need to study in this sector.
3. Develop a proposed vision for the concept of cybersecurity and its role in improving risk management in the Iraqi tourism sector in general and at Baghdad International Airport in particular.
4. Concept of Cybersecurity requires more scientific research and explanatory studies, and to be the study as a new entrance in our time, it is not one of the modern trends in various service organizations of a tourist nature.

Problem of Research: The problem arises from the limited application of cybersecurity at Baghdad International Airport, especially being the civilized interface of the country and the main gateway to our tourism sector and the interspersed uses and applications of complex software and electronic systems, as well as the definition of risk management in the place of research application is still primitive, and for this it needs to bridge the research gap and its repercussions on achieving success in that management, as well as the adoption of cybersecurity to develop risk management and achieve excellence and success in the work of the airport in light of the capabilities Available and attention paid by the Council of Ministers, that the increasing problems faced by airports and its administrative apparatus in its management of risks related to the information system, navigation systems and forms of electronic reservation, and as a result of the rapid information revolution in the development of the cybersecurity environment, and the great responsibility that falls on the shoulders of the airport management in general and the management of cybersecurity and risk management made researchers raise a major question (Was Baghdad International Airport able to adopt cybersecurity in improving its risk management?), as well as the application level for the search variables.

The study adopted the following main hypotheses: - To solve problem of research and choose main hypothesis, a field study was conducted at Baghdad International Airport and the study sample was the departments and at the three levels, since it is an essential point in improving Risk Management, specialized interviews with Information Security Department and the Risk Management Division in it have contributed to some phrases that determine the level of application of cybersecurity and make risk management play its responsible role in front of higher authorities, passengers, international airlines and suppliers of airlines Local and international aviation that use Baghdad Airport and according to the main hypothesis (there is no statistically significant impact of cybersecurity in improving risk management at Baghdad International Airport at the significance level of 0.05.($\partial \leq 0$).

1.1. Objectives

1. Knowledge of the theoretical and intellectual aspects of the concept of cybersecurity and risk management.
2. Identify the level of application of cybersecurity and risk management by determining their dimensions at Baghdad International Airport.
3. Identify the impact of cybersecurity and its dimensions in risk management.
4. Reaching some proposed conclusions and recommendations to enable airport management to improve risk management and cybersecurity management.

1.2. Research Limits

1. Time limits, the study was implemented in 2024-2025.
2. Spatial boundaries, study population and designated by the State Company of Iraqi Airways.

Research Methodology: The research adopted the descriptive statistical analysis methodology.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 3123-3134, 2025
DOI: 10.55214/25768484.v9i4.6743

1.3. Sources of Information Collection

1. Primary sources, from statistical data of study sample through "study management" questionnaire.
2. Secondary sources, including the knowledge library of sources, books, magazines, conferences, the Internet and some previous studies.

2. Theoretical Aspect

2.1. Cyber Security

2.1.1. Concept and Importance of Cybersecurity

Cybersecurity is part of national security, which includes the protection of critical infrastructure, and others see it as the protection of personal data and ensuring the confidentiality of information, and there are those who look at cybersecurity from a purely technical perspective, as it looks at a set of tools and techniques used to address cyber threats, andthis variation reflects the diversity and development of the field continuously [1, 2] while controlling access to data systems connected through networks and controlling the information contained in them [3] and on this basis cybersecurity has become a set of measures aimed at protecting against various types of attacks that lead to unauthorized access to the organization's information. (hardware, networks, software) or alteration or destruction of their consequences as well as the information systems of associated personnel [2] from Guiora's point of view [4] constitutes the protection of information, communications and technology from damage caused either accidentally or intentionally. It is important to emphasize that a cyber-attack is profoundly different from a physical attack, as is the effort to ensure the confidentiality, integrity and availability of data, resources and operations from Through the use of administrative, physical, and technical controls, what Kremling and Parker [5] sees as the organization and aggregation of resources, processes, and structures used to protect cyberspace and systems supported by cyberspace from events that conflict by law with actual property rights.

On this basis, cybersecurity has become a computing-based system that includes technology, people, information and processes to enable confirmed operations. It involves the creation, operation, analysis and testing of secure computer systems [6] and is described as the process of preventing data loss or sabotage by closing all possible avenues of attack by exploiting cyber vulnerabilities to ensure confidentiality and not loss or damage to information [7].

Internet networks and information technology have created opportunities for the global economy and community networking in the world. However, reliance on this technology has exposed vulnerabilities through the many cyber activities of state and non-state actors, public and private companies, as well as government agencies, including air traffic control systems, electric power grid, communication networks, and financial systems. As a victim of cyber-attacks. Critical infrastructure by a group of hackers and criminals, and the more reliance on information technology in administrative and financial transactions, the motives for cyber-attack continue to rise [8] as cybersecurity plays a vital role in securing data such as social media accounts, credit card numbers, cloud storage services, etc., as misuse of the Internet has become a problem. In various sectors of life, especially in social media and government institutions, the role of cybersecurity has emerged as one specific, security environment and subsystem of national security at the state level, is a system of continuous and planned increase of political, legal, economic, security, defense and educational awareness, including also the efficiency of risk control measures adopted and applied of a regulatory technical nature in cyberspace in order to transform them into a trustworthy environment that provides safe operation. For socio-economic processes with an acceptable level of risk in cyberspace [9] cybersecurity ensures the preservation of the organization's security characteristics and protection against security risks within the cyber environment, Internet threats have become more complex as computer systems become increasingly integrated or interconnected, and the number of cyberattacks is constantly increasing, and therefore the sense of urgency to develop trends increases. and new security guidelines and practices to counter cyber risks around the world [10] thus including the importance of cybersecurity [11] in improving

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 3123-3134, 2025
DOI: 10.55214/25768484.v9i4.6743

cyberspace security, increasing cyber defense, increasing Internet speed, protecting data and information for organizations, and also provides protection systems against viruses, worms, malware, spyware, etc., as well as protecting personal privacy, protecting networks, data and storage resources. Anti-hackers and identity theft for computer system.

2.1.2. Dimensions of Cybersecurity

Cybersecurity is related to several diverse areas, including aspects (political, military, economic, legal, and social) and with the aim of building a comprehensive system aimed at protecting the national security of the state from any potential cyber threats [12] and some countries have expanded the concept of cybersecurity to include important additional dimensions such as the intelligence, media, and strategic dimensions, and other dimensions that the researcher will address later in detail [13].

A. Political dimension: political dimension focuses on the state's responsibility to achieve cyber (digital) security, and by protecting its political system by establishing a unified and effective legal framework, state's efforts should not only be focused on supporting research and development in field of security, but should go beyond that to promote a security culture and adhere to minimum security standards, and law enforcement with regard to cybercrime [14] on the other hand, political actors benefit greatly from modern technologies to reach the widest possible segment of citizens and promote their policies, regardless of the validity of those policies or principles they promote. For example, former US President Barack Obama used social media extensively during his election campaign. On the other hand, leaks of thousands of classified diplomatic documents via WikiLeaks have had a negative impact on diplomatic relations between countries and their credibility [15].

B. The economic dimension: Cyberspace has become a focus of attraction for various groups of society, whether individuals or groups, as it depends mainly on digital technology in storing data and information, and the computer is used in the development of industries and moving the wheel of the economy, as financial and economic transactions have turned into computerized systems, and networks of banks, stock exchanges and financial market companies have become connected through electronic systems and networks, making the Internet a fundamental pillar for financial and economic transactions, and one of the According to a report issued by E-Marketer, the volume of e-commerce reached $ 1.5 trillion in 2014, a significant increase compared to 2013, when it reached $ 1.2 trillion. With the rise in cybercrime, the digital economy of countries is threatened, highlighting the need to implement cybersecurity [12].

C. protecting information: McAfee, a global company specialized in software and cybersecurity systems, indicated in its report on the list of countries most prepared to address piracy, cyberespionage and data protection, the superiority of European countries in this field. These countries have established a "cyber force" to counter threats to critical infrastructure [13] as well as protect the confidentiality of sensitive information. From the access of strangers to it, and the protection of the integrity of information, as it should be protected from unauthorized change or deletion, in addition to the protection of the availability of information and its availability when needed by beneficiaries, and protection from electronic threats and be protected from electronic threats such as viruses and malware, and protection from unauthorized access, that is, be protected from unauthorized access by unauthorized persons [16].

D. Legal dimension: Individual, institutional and governmental activities in cyberspace have legal effects that require the attention of the competent authorities to develop rules for resolving potential disputes, as the changes that accompanied the emergence of the information society should be taken into account, in addition to the fundamental rights and human freedoms recognized in constitutions and international laws, new rights have been added, such as the right to access the World Wide Web, and some concepts have expanded to include new practices such as the creation of blogs and online gatherings, Protection of software intellectual property rights [15] and the relationship between law and technology is a reciprocal relationship, and technological developments force legislation to keep pace with it by developing legal frameworks that regulate legal and illegal actions, as cybercrime still

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 3123-3134, 2025
DOI: 10.55214/25768484.v9i4.6743

lacks more stringent aspects to deal with it, due to its complex nature and the difficulty of identifying perpetrators of cybercrime, in addition to that The flexibility of definitions related to information technology and the non-compliance of cybercrimes with state borders pushes countries to cooperate jointly in confronting these crimes [12].

E. Social dimension: Cyberspace and through blogs and social networking sites in particular, allows individuals the opportunity to express their political aspirations and social ambitions in a variety of forms, and this space rich in ideas and opinions contributes to the enrichment and development of society through the exchange of diverse ideas and information, and the ability of the Internet to transfer these aspirations and ideas and scientific, cultural and service services to various parts of the world and to specific groups such as the elderly and the sick The Internet plays an important role in the exchange of information during disasters and humanitarian situations, allowing aid to reach quickly, and social impact goes beyond the comfort limits provided by the Internet, to reach the benefit of information and communication technologies in supporting various community activities, while preserving basic values such as belonging, beliefs and traditions through the establishment of groups aimed at spreading awareness among members of society [15]. The need to provide security and hold individuals personally liable, along with taking the deterrent measures provided for in the Criminal Code for those who do not comply with security requirements, must be emphasized. More generally, it becomes necessary to provide ICT education and training, especially with regard to security education and how to safely use ICT. The global information network should remain an open space for all. Can benefit from the infrastructure and services available to them without being exposed to excessive security risks [14].

F. Military dimension: Comparative advantage of cyber power is its ability to connect military units via military networks in cyberspace, facilitating rapid exchange of information, enabling the efficient flow of military commands, and enabling the ability to remotely control and hit and destroy targets. However, this feature may turn into a vulnerability if the electronic network used is not adequately secured against external intrusions, These attacks may lead to destruction of military databases, disrupt the state's ability to deploy its forces quickly, cut off communication systems between military units and paralyze computer networks, disable enemy air defense systems or electronic guidance, and even lose control of command and guidance units, which may lead to the enemy's inability to control satellites [12].

Examples of such breakthroughs include incidents in Brazil and the United Kingdom, where energy infrastructure was compromised, resulting in power outages and affecting millions of people and institutions [15].

1. Educational and academic dimension: Cyberspace has been included in the curricula of universities, especially in fields of information systems engineering and computer science, as the topics covered by the curriculum focused on methods of detecting cyber-attacks, protection against viruses and malware, and securing networks and operating systems [13] and this type of activity is known as "ethical hacking", and represents Non-violent use of technology to achieve certain goals, whether political or non-political, and these goals are often legally and morally controversial. Ethical hackers aim to discover vulnerabilities in computer systems in order to enhance their security and protection from external intrusions [17].

2.2. Risk Management

2.2.1. Concept and Importance of Risk Management

Risk management embodies " state of uncertainty, suspicion or fear of the realization of a particular phenomenon or situation" [18] and therefore a relationship between risk and uncertainty is complementary if organization does not recognize environmental survey methods, so it is considered "measurable uncertainty" [19] so risk is an actual state that can be measured by determining the probability of its occurrence, while uncertainty is "a state of mind in individuals that means the inability to know results and thus be unmeasurable" [20] it is an integral part of organizational processes and

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 3123-3134, 2025
DOI: 10.55214/25768484.v9i4.6743

part of the decision-making process, as provided by the Association of Insurance and Risk Managers in Industry and Commerce (AIRMIC) is a functional description of organizational risk management as a management tool that enables an organization to lead a formal process to continuously improve its risk control capabilities in a changing business environment. Other characteristics in the literature include describing it as a comprehensive and powerful risk management tool [21], so I considered a systematic approach to managing uncertainties that could pose a threat and assessing risks by developing all strategies to mitigate those risks using resource management or empowerment, as well as improving the image of the internal and external organization [22] and from another point of view considered possibility of loss or unexpected result associated with an action, and uncertainty here represents the lack of knowledge of what will happen in the future, and the greater the uncertainty, a greater the risk for the organization, risk management involves improving the expected returns according to risks involved and risk tolerance [23]. Finally, risk management is an integrated organization aimed at confronting risks with best means and lowest costs by detecting, analyzing and measuring these risks and determining the means to confront them, as well as choosing the most appropriate means to achieve the desired goal [24].

Risk management gives the organization the ability to absorb risk levels and benefit to reduce inefficiencies necessary in order to increase efficiency of its performance in a way that allows enhancing internal communication and reducing information discrepancies, which helps in refining the decision-making process, and also helps to align risks with its strategy and improve response to them, leading to reducing losses, for this reason it can get alignment Between risk and long-term performance, risk management can reduce cost of hedging risk by preventing the recurrence of hedging and focusing exclusively on residual risks and contribute to reducing the costs associated with risk handling, which represent the efforts being made to identify options that would limit or minimize the impact of risk [25] and from another angle explain [26] Benefits for risk management include increasing the likelihood of achieving objectives, proactively identifying and addressing risks, improving governance, stakeholder trust, establishing a foundation for decision-making and planning for the future, allocating and using resources effectively, improving effectiveness, efficiency and safety, enhancing health and safety performance and protecting the environment, reducing losses and maximizing return on investment.

2.2.2. Dimensions of Risk Management

Risk management includes the application of policies, procedures and practices for communication and consultation activities, identifying and assessing risks and then addressing, monitoring, reviewing and reporting them [27] as risk management represents a scientific and systematic approach to dealing with risks, it has become going through a logical series of steps that can be clarified through the following: [28, 29].

1. Goal setting: It represents the first step in the risk management program to obtain the maximum benefit from the expenses associated with risk management should develop a precise plan, for example, low cost may be a primary goal of risk management, but focusing on the cost element may result in following an insufficient or inappropriate risk management program, and this may result in incurring very large costs resulting from the large losses that the organization can bear under an insufficient or insufficient program Appropriate, therefore, primary objective of risk management should be to protect all the activities of the organization from any risks or expected losses that limit the achievement of objectives.

2. Risk detection: Risk management in the organization seeks to study and analyze activities in order to discover risks that organization expects to face in stages of its activities by answering the questions: What is expected risk? How likely is it happening? How dangerous is it happening? What actions need to be taken to reduce the likelihood of their occurrence, or to minimize the consequences?

3. Risk assessment: After identifying and discovering risks, organization should evaluate them by measuring the potential size of the loss and the probability of its occurrence, and the risk assessment is conducted systematically and participatory based on the experiences and opinions of stakeholders, using

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 3123-3134, 2025
DOI: 10.55214/25768484.v9i4.6743

the best available information, with more inquiry, and it must arrange and develop a risk classification because there are risks that the severity of the potential loss is greater than risks Other, and in most cases, there will be a number of risks that require equal attention.

4. Identifying alternatives and choosing the best alternative to face the risk: After identifying and analyzing the risks, optimal option should be determined to face risks, and the stage of identifying alternatives is stage of deciding on the best means available in dealing with risks, and to make a specific decision to face certain risks, risk management officer takes into account Consideration of the probability of loss and resources available to face risk, and decisions can be made in which the benefits or advantages exceed the costs, and the more accurate choice of means of assistance in the face of the risk, greater efficiency and effectiveness in face and resistance to risks, that is, making appropriate decision in right place.

5. Implementation of a decision: After decision is made, an implementation stage comes, whether decision is to transfer the risk to another party, face the danger and reduce its impact, or escape from it through the least losses.

6. Evaluation and Review: Evaluation and review should be included in risk management program for two reasons: First: that risk management process does not take place in a vacuum as things change and new risks arise and other risks disappear, so techniques that were appropriate in past may not be optimal in present and future, which requires the need for continuous and continuous attention, and the second: dangers sometimes occur without paying attention to them, as Conducting an evaluation and review of risk management programs allows the discovery of these risks, including correcting decisions before they become expensive and losses, and although risk manager must evaluate and review as important functions that must be done, we find that some organizations use independent consultants periodically to review and evaluate their programs, but this does not prevent the organization from need to find internal means and policies, working to manage the risk management process and reduce losses to the maximum extent possible.

3. Practical Side of Statistical Analysis

Third section dealt with applied aspect of research of study and its tool to collect main data "questionnaire" and its axes and how it was developed in addition to community and sampled, and method used to reach sincerity of "questionnaire" and stability, and statistical processes parameter about data answered by sample when surveyed.

Research Approach: descriptive analytical approach was adopted, because it is an organized approach to study of the human and social phenomenon away from emotional feelings of the two yards, as the answers of individuals of the sample are filled and analyzed to find relationship between its variables, using appropriate statistical analysis, which is as follows multiple regression to indicate the impact of cybersecurity and its dimensions as an explanatory variable in improving risk management as an approved variable, and from point of view of management at organizational levels of Baghdad International Airport.

Population and Sample: Size of total community according to model (D. MORGIN), amounted to (87) managers, head of department and official division and unit at Baghdad International Airport and according to organizational structure, and a random sample was selected amounting to (71), and (67) questionnaires were retrieved, all of which are valid for statistical analysis, and using the Spss V.28 program to analyze answers of the sample members

Validity and stability of "questionnaire": sincerity of research tool questionnaire a possibility of measuring what was designed from solution, and its apparent sincerity was verified by presenting it to the arbitrators to verify the sincerity of its phrase and clarity and the possibility of measuring the required and integrity of formulation of its phrase linguistically.

validity and access to same results in event of repeating measurement process for several times, and the researchers adopted method of alpha Kronbach to measure extent of internal consistency of its phrases and to verify stability of resolution and results were as shown in Table 1 as it is clear value of

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 3123-3134, 2025
DOI: 10.55214/25768484.v9i4.6743

stability and honesty of resolution and enjoyment of statements of independent variable with a high level of stability and honesty by (0.877), and that the dependent variable got value of Cronbach coefficient alpha (0.901), while resolution in its total form got alpha coefficient of Cronbach (0.923).

Table 1.
Measurement of resolution stability.

Cronbach's alpha coefficient	Variables
0.877	Cyber Security
0.901	Risk Management
0.923	Total

Source: Prepared by researchers according to the results of the analysis of the SPSS v.28.

Descriptive statistics of variables and their dimensions: Table 2 shows mean, standard deviations, coefficient of variation for cybersecurity and its dimensions, as well as risk management and their dimensions, in terms of their availability of strength and weakness, with order of priority of application at Baghdad International Airport

Table 2.
Descriptive Statistics of Variables and their Dimensions.

Variables	Mean	St. d	C. V	Priority
Cybersecurity	4.26	0.428	10	FIRST
Political	4.22	0.844	11.4	2
Economical	4.11	0.588	14.3	6
Protect of Information	4.24	0.585	13.8	5
Legal	4.30	0.546	12.7	4
Military	4.43	0.469	10.6	1
Academic and Educational	4.25	0.519	12.2	3
Risk Management	3.58	0.459	12.8	SECOND
Goal setting	3.88	0.432	11.1	4
Risk detection	3.65	0.354	9.7	2
Risk assessment	3.28	0.315	9.6	1
Identifying alternatives and choosing best alternative	3.92	0.402	10.2	3
Implementation of a decision	3.34	0.512	15.3	5
Evaluation and Review	3.38	0.551	16.3	6

Source: SPSS V.28.

The explanatory variable cybersecurity practice and availability at Baghdad International Airport obtained a mean (4.26) and a standard deviation of (0.428), indicating the adoption of airport management and its various organizational levels Protection of computers, servers, mobile devices, electronic systems, networks and data from malicious attacks and information technology security or electronic information security is high, which made coefficient of variation (10%), which indicates agreement (90%) of the sample on this behavior and to prioritize it in A first place.

The military dimension got the priority of agreement by a research sample and with a relative coefficient of variation (10.60%), as it was adopted by the airport management with a very high mean (4.43), while political dimension ranked second and a coefficient of variation coefficient (11.40%), while educational academic dimension ranked third with an mean (4.25) and a coefficient of variation (12.2%), while legal dimension was in a priority of an airport management fourth and a coefficient of variation (12.7%) and a mean (4.30) high practice and interest, while solution after information protection ranked fifth and with a coefficient of variation (13.80%) and practice with a mean (4.24), and finally solved economic dimension of cybersecurity in sixth order and a relative coefficient of difference (14.3%) and availability with a mean (4.11), this very high level of attention to six dimensions has made cybersecurity a top priority by applying at the expense of the other variable.

The significant risk management variable ranked second in terms of the priority of agreement by a research sample with a coefficient of variation (12.8%) and a high a mean (3.58) through adoption of an

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 3123-3134, 2025
DOI: 10.55214/25768484.v9i4.6743

airport management process of measuring and evaluating risks and developing strategies to manage them, as these strategies include transferring risks to another party, avoiding them, reducing their negative effects, and accepting some or all of their consequences .At level of dimensions, after assessing risks, it obtained the first rank with a coefficient of variation (9.6%) and a mean (3.28) available but does not meet an ambition of sample, while it came after determining risks second and with a relative coefficient of variation (9.70%) and a mean (3.65), while airport management took to identify alternatives and choose the best one in a third order and with a mean (3.92) and a coefficient of variation (10.2%)As for setting goal, a priority of an airport management was ranked fourth and with a coefficient of variation (11.1%) and availability with a mean (3.88) high, while an airport management tended to implement a decision in the fifth order and with a coefficient of variation (15.3%) and a mean (3.34), and finally after evaluation and review the sixth rank and with a coefficient of variation (16.3%) and a mean (3.38) available and receives average attention from point of view of a sample.

3.1. Testing the Main Research Hypothesis

In order to verify the main hypothesis "there is no statistically significant impact of cybersecurity in improving risk management at Baghdad International Airport at the significance level of 0.05.($\partial \leq 0$)". To know the level of impediment between risk management and an interpreted dimension, represented by dimensions of Cybersecurity, using multiple linear regression as shown in Table 3 which were classified as explanatory variables, namely (cybersecurity dimensions) and the risk management variable as a dependent variable.

Table 3.
Shows impact of cybersecurity on risk management.

Risk Management							
F	**β**	**R²**	**AJ R²**	**T**	**P**	**α**	**Variable**
9.858	0.264	0.36	0.324	1.813	0.074	1.527	Political
	0.445			2.618	0.011		Economical
	0.456			2.879	0.005		Protect of Information
	0.315			2.5	0.015		Legal
	0.096			1.535	0.105		Military
	0.084			0.981	0.251		Academic and Educational

Source: SPSS v.28.

It was clear from results of Table 3 that a value of (F = 9.858) calculated for model at degrees of freedom (6,60,55) was higher than a tabular value (3.984) and with a degree of freedom (66), which supports an acceptance of alternative hypothesis (H1) and rejection of null hypothesis (H0) (there is no statistically significant effect of cybersecurity in improving risk management at Baghdad International Airport at the significance level of 0.05). $\partial \leq 0$)).

As a model (32.4%) explained changes that occur in Risk Management and are attributed to Cybersecurity, as the model is good in interpreting (RM) by Cybersecurity model adopted by research, while remaining percentage (67.6%) is attributed to other variables that did not fall within current model of the research, as a management of Baghdad International Airport adopted Cybersecurity in general and especially their dimensions of Economic , Legal and dimension of Information Protection in improving the level of (RM), while Political, Military and Academic Educational dimension was not adopted on improving a level of risk management in Baghdad International Airport.

While it was found that the committees of the Iraqi Council of Representatives adopted an Economic dimension and increased Risk Management by (44.5%) and value of (T = 2.618) calculated, as well as the impact of Information Protection by (31.5%) and value of (T = 2.500) calculated, while the impact of the Legal dimension was positive and by (45.6%) and the value of (T = 2.879).), all calculated T values were above their tabular value (1.996) at the degree of freedom (66), while Baghdad

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 3123-3134, 2025
DOI: 10.55214/25768484.v9i4.6743

International Airport management was unable to employ other dimensions to improve its risk management.

4. Conclusions and Discussion of Results

In a light of field results (cybersecurity and its impact on improving risk management at Baghdad International Airport), the research reached the following conclusions.

The research confirmed the level of interest and encouragement of management of Baghdad International Airport in cyber security, which called for it to build indicators related to policies and procedures that are highly interested in a future of an airport from this perspective, as well as adopting ideas that increase the safety of creative work policies and contribute to building the airport's reputation locally and globally, and this is what made its economic orientations towards building a cybersecurity system, as it is one of the factors that stabilize the airport's work It enhances its ability to catch up with technological progress, and drive economic activity and growth, which is achieved through communication and information technology applications such as travel, electronic ticketing, financial transactions with airlines and e-government, and there is no doubt that cybersecurity has a very important role in the economy, with the continued technological progress and the increasing adoption of air and tourism transport companies On digital platforms, the risk of cyber threats is becoming more widespread, and cyber-attacks can have serious consequences for their operation, causing financial losses, defamation, and even breaches of national security. By controlling airports and paralyzing air traffic, it is essential that governments, airports and individuals give top priority to cybersecurity measures to protect their interests., which is related to the protection of information, as well as the development of regulations, compliance with laws, the installation of rights to intellectual property and software, the use of specialized work teams, communication with universities, building bridges of knowledge, exchanging information and the use of specialized professors made cybersecurity at Baghdad International Airport available with high interest and sample agreement.

The research found that there are some weaknesses in sub-aspects associated with one of the dimensions of risk management, and this reflects the need to research and highlight the important aspects of the process of identifying, analyzing and reducing potential threats that may affect the safety and security of air operations, as this management aims to ensure a safe environment for passengers and workers and protect the infrastructure from potential risks, as it shows the ability of airport risk management Identify all potential risks such as air accidents, natural disasters, security threats, cyber-attacks, and assess the probability of each risk and its impact on the operations carried out by the airport management, but this role did not win the approval of the eye and realized that its practice is weak and needs committees and work teams specialized in evaluating it, knowing that the airport management has proven its high ability to develop contingency plans and strategies to reduce the impact of risks, such as evacuation plans and dealing with crises Cooperation with security authorities and airlines, training airport staff to deal with emergency situations and promote a culture of safety, as it has been proven to apply advanced surveillance and security systems, such as surveillance cameras, baggage screening devices, and hazardous materials detection systems, working with government agencies, airlines, and security services to ensure an effective response to risks As the airport took it upon itself to put forward a lot of alternatives, and as a result it took decisions implemented to some extent, as the sample realized that the implementation of development decisions still needs a lot, and that evaluation and review are still in the stage of emerging beginnings that do not meet the ambition, so the management of Baghdad International Airport tended to use cybersecurity in risk management through the economic dimension, information protection and the legal dimension correctly, accurately and statistically proven through the results of Current search.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 3123-3134, 2025
DOI: 10.55214/25768484.v9i4.6743

Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

References

[1] W. Smith, "A comprehensive cybersecurity defense framework for large organizations," Doctoral Dissertation, ProQuest Dissertations Publishing, 2019.

[2] T. A. Johnson, *Cybersecurity protecting critical infrastructures from cyber attack and cyber warfare*. USA: Taylor and Francis Group, 2015.

[3] J. L. Bayuk, P. Healey, J. Rohmeyer, M. H. Sachs, J. Schmidt, and J. Wiess, *Cyber security policy guidebook*. Hoboken, NJ: John Wiley & Sons, Inc, 2012.

[4] A. N. Guiora, *Cybersecurity: Geopolitics, law, and policy*. New York: Crc Press, Routledge, 2017.

[5] J. Kremling and A. M. S. Parker, *Cyberspace, cybersecurity, and cybercrime*. California: Sage Publications, 2018.

[6] W. J. Caelli, *History and philosophy of cyber security education. In G. Austin (Ed.), Cyber security education: Principles and policies*. London, United Kingdom: Routledge, 2020.

[7] A. Kohnke, D. Shoemaker, and K. Sigler, *The complete guide to cyber security risks and controls*. USA: Taylor And Francis Group, 2016.

[8] J. Callen-Naviglia and J. James, "Fintech, regtech, and the importance of cybersecurity," *Issues in Information Systems*, vol. 19, no. 3, pp. 220–225, 2018. https://doi.org/10.48009/3_iis_2018_220-225

[9] P. Losonczi, "Importance of dealing with cybersecurity challenges and cybercrime in the senior population," *Security Dimensions. International and National Studies*, vol. 26, pp. 173-186, 2018.

[10] R. Rondelez, "Governing cyber security through networks: An analysis of cyber security coordination in Belgium," *International Journal of Cyber Criminology*, vol. 12, no. 1, pp. 300–315, 2018. https://doi.org/10.5281/zenodo.1467929

[11] H. A. Hussein, "Cybercrime and the challenges of global policing," *Legal and Political Sciences*, vol. 12, no. 1, pp. 1-10, 2020.

[12] M. Muhammad, "Cyber security," *Future Concepts, Event Trends*, vol. 6, no. 1, pp. 1-10, 2015.

[13] M. Yahya, "Measuring speaking anxiety among speech communication course students at the Arab American University of Jenin," *European Social Sciences Research Journal*, vol. 1, no. 3, pp. 229–248, 2013.

[14] International Telecommunication Union, *A guide to useful cybersecurity law*. Geneva: International Telecommunication Union, 2007.

[15] M. A.-A. Jbour, *Cybersecurity: The barrier of the age*. Beirut: Arab League - Arab Center for Legal and Judicial Research, 2016.

[16] ISO 27001, *Information security management system*. Geneva: International Organization for Standardization, 2018.

[17] T. Maurushat and R. Morgus, *Compilation of existing definitions related to cybersecurity and information security*. Switzerland Federal Department of Foreign Affairs, 2019.

[18] E. A. Abu Bakr and W. I. Al-Sayfo, *Risk management and insurance*, 1st ed. Amman, Jordan: Al-Yazouri Scientific House for Publishing and Distribution, 2009.

[19] C. M. Harvett, "A study of uncertainty and risk management practice relative to perceived project complexity," Doctor Of Philosophy, Bond University, Harvett Cm, 2013.

[20] A.-K. M. Quinn, "Using risk measures with a focus on scenario-based models in asset risk assessment ", Unpublished Ph.D. In Business Administration, College Of Administration And Economics, Al-Mustansiriya University, 2013.

[21] K.-B. Oh, C.-T. B. Ho, and B. Slade, *Cybersecurity risk management: An enterprise risk management approach*. New York: Nova Science Publishers, 2022.

[22] J. S. Suroso and M. A. Fakhrozi, "Assessment of information system risk management with octave allegro at education institution," *Procedia Computer Science*, vol. 135, pp. 202-213, 2018. https://doi.org/10.1016/j.procs.2018.08.167

[23] F. Laurens, "Basel III and prudent risk management in banking: Continuing the cycle of fixing past crises," *Risk Governance & Control: Financial Markets & Institutions*, vol. 2, no. 3, pp. 17-22, 2012.

[24] A. E. Salam and S. N. Musa, *Risk management and insurance*. Sudan: Hamid Publishing and Distribution House, 2007.

[25] A. A. B. A. Wiradarma and G. M. A. Sasmita, "It risk management based on iso 31000 and owasp framework using osint at the information gathering stage (case study: X company)," *International Journal of Computer Network and Information Security*, vol. 9, no. 12, pp. 17–29, 2019. https://doi.org/10.5815/ijcnis.2019.12.03

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 3123-3134, 2025
DOI: 10.55214/25768484.v9i4.6743

[26] M. P. Thompson, D. G. Macgregor, and D. E. Calkin, *Risk management: Core principles and practices, and their relevance to wildland fire*. Fort Collins, CO, USA: U.S. Department of Agriculture, Forest Service, Rocky Mountain Research Station, 2016.

[27] K. Kapsa, "Risk management in biogas plants based on new norm ISO 31000: 2018," *Transport Economics and Logistics*, vol. 77, pp. 59-72, 2018.

[28] J. A. Theodorou and I. Tzovenis, "A framework for risk analysis of the shellfish aquaculture: The case of the Mediterranean mussel farming in Greece," *Aquaculture and Fisheries*, vol. 8, no. 4, pp. 375-384, 2023. https://doi.org/10.1016/j.aaf.2021.04.002

[29] M. Dallas and A. P. M. Director, *Management of risk: Guidance for practitioners and the international standard on risk management, ISO 31000: 2009*. London: The British Standards Institution, 2013.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 4: 3123-3134, 2025
DOI: 10.55214/25768484.v9i4.6743