Volume 04, Issue 01, 2024,
Publish Date: 19-02-2024
Doi https://doi.org/10.55640/ijthm-04-01-01

INTERNATIONAL JOURNAL OF TOURISM AND HOSPITALITY MANAGEMENT (Open access)

The Role of Cybersecurity in Facing Technological Challenges in Tourism Companies in Baghdad

Zainab Abad Alrada Al moussawi[1]

[1]Ahl AL-Bayt Univerisy
(zainabalmoussawiii@gmail.com)

ABSTRACT

Tourism agencies are among the business organizations that use e-commerce. In light of the increasing risks of technological challenges and cyber threats, focusing on cyber security requirements has become essential. From this standpoint, the study aimed to define the concept of cyber security and its importance, identify its dimensions and requirements, and demonstrate the impact of cyber security in Addressing technological challenges in tourism agencies. The study relied on the descriptive analytical approach and used a questionnaire to collect study data from a random sample of workers in tourism agencies in Baghdad, numbering (110) individuals. The study found statistically significant differences between the opinions of the study sample about the role of cybersecurity in confronting technological challenges. Tourism agencies in the city of Baghdad, and the presence of a statistically significant effect of cybersecurity on facing technological challenges in tourism agencies in Baghdad. The study recommended the necessity of activating the role of the response team to cyber events in Iraq, establishing a special department for information security in tourism agencies, and qualifying tourism human resources to deal with cyber technological threats.

KEYWORDS: Cyber security, Technological challenges, Tourism agencies and Baghdad.

INTRODUCTION

Tourism companies have steadily increased their reliance on digital technology and building electronic information bases, which help customers and tourists learn about the various elements of the tourism program, identify appropriate tourist destinations, and complete the purchase of tourist trips through the Internet (Al-Basri and Hassan, 2021, p. 339). The tourism sector has become the most used of digital technology, representing 40% of e-commerce uses globally (Lakhal et al., 2022, p. 341). No doubt drawing the attention of senior management in tourism companies to the risks of technological challenges and cyber threats must be taken into consideration due to the increasing severity of Security risks related to cybersecurity and how to activate cyber protection systems and implement control, control and monitoring processes within the framework of a solid plan that ensures the success of the information security department in formulating a cybersecurity strategy to improve the efficiency of information circulation and its integration and protect its privacy from inside and outside the organization (Qaddaifah, 2016, p. 160).

Hence, the current research focuses on the role of cybersecurity in confronting technological challenges in tourism companies in Baghdad.

First - The methodological framework:

1. Problem of the Study

The problem of the study is that Iraq is exposed to many security problems related to cyberspace, and this is due to the absence of security and political stability, the weakness of the material and human capabilities, and the technological techniques necessary to address cyber risks, which affects the efficiency of business organizations in Iraq to deal effectively with these problems. It exposes these organizations to various cyber risks (Khuresan, 2021, p. 8). From this standpoint, the issue of the study is embodied in answering the following question:

How does cybersecurity contribute to facing technological challenges in tourism companies in Baghdad?

2. Hypotheses of the Study

First hypothesis:

"There are statistically significant differences between the opinions of the study sample about the role of cybersecurity in confronting technological challenges in tourism companies in Baghdad."

Second hypothesis:

"There is a statistically significant effect of cybersecurity on facing technological challenges in tourism companies in Baghdad."

3. Objectives of the study:

Defining the concept of cybersecurity and its importance.

Identify the types and dimensions of cybersecurity in tourism companies.

Identify the most important technological challenges for tourism companies.

Reviewing cybersecurity efforts and requirements in tourism companies

Statement of the impact of cybersecurity in addressing technological challenges in tourism companies in the city of Baghdad.

4. Limitations of the study

Methodological limitations: The study relied on the descriptive analytical approach and the applied survey approach by depending on the questionnaire as the primary tool for collecting study data.

Spatial boundaries: The applied aspect of the research concerns tourism companies in Baghdad, Iraq.

Time limits: The questionnaire was distributed via the Internet (Google Forms) from 10/1/2023 to 12/15/2023 AD.

Human Limits: The research is concerned with surveying the opinions of a random sample of workers in tourism companies in Baghdad, amounting to (110) individuals.

Theoretical framework

1. The concept of cyber security:

The American mathematician Norbert Winner

used the word cyber for the first time in 1948 to explain the feedback system, which depends on the systems' outputs to adjust and control the inputs (Atiyah, 2019, p. 103).

Since the advent of computer viruses in 1988 by Robert Morris, who published the first virus on the internet and was able to infect about 6,000 personal computers connected to the internet, the United States of America has begun to form a team dedicated to dealing with cases of computer hacking, and the European Union has enacted legislation and laws to combat cybercrime related to the internet (Chalabi & Ahmed, 2009, p. 207), and this was the beginning of the emergence of the concept of cybersecurity, which and technology) in the United States of America as The ability, activity, or operation aimed at protecting information and communication systems, associated data, and information, and protecting them from hacking or illegal exploitation, or the possibility of damaging or damaging them (NATO, 2016, p.17).

Cybersecurity refers to various means, methods, and mechanisms that are used to counter all forms of electronic attacks that computers (rumbling Ware), as well as information and communication networks, software (software), detect and monitor viruses, deal with them and prevent them from affecting hardware and software (Amoroso, 2007, p.1), it also means the security field related to the protection of information systems, networks and data and taking the necessary measures to address electronic threats via the internet and face their effects (al-dalabih, 2021, P.5), it is also defined as administrative, organizational and operational means and techniques that seek to counter various illegal, or unauthorized uses of electronic data and information, or retrieval and use for other than the purposes intended for them, and to provide means of privacy, protection and confidentiality of electronic data to national and private organizations and individuals (al-January, 2021, the P. 81).

2. the importance of cybersecurity for tourism companies:

The importance of cybersecurity in tourism companies is as follows:

- Providing electronic systems for the protection of electronic information on computers and the protection of software operating them to prevent their penetration by unauthorized persons or entities at the individual, institutional, and national levels (mashosh, 2018, P.50).
- Many countries rely on unified digital infrastructure networks linked to cyberspace within the framework of the National Information Infrastructure, which serves all vital sectors in the country, such as e-commerce, financial exchanges, communication systems, Government Services, Energy Management, and transport, which necessitates their protection through the provision of cybersecurity systems (Belford, 2016, p.149).
- Monitoring and neutralizing targeted or potential cyber-attacks and breaches and applying modern technological technologies for cybersecurity before they reach private and Government Information Systems (Al-jumusi, 2016, P.120).
- The spread of the risks of electronic globalization, in light of the intensive use of digital information in all aspects of public and professional life and the growing use of computers and smartphones, requires the application of cybersecurity systems (Khodari et al., 2020, p. 222).
- Filling gaps in vulnerabilities in data, information, and computer security systems of all kinds through the provision of cyber security systems (Al-Samhan, 2020, p. 12).
- Achieving information and communication security at the individual and institutional levels, maintaining its privacy and confidentiality, limiting dealing with it to authorized persons using it, and Combating Cybercrimes (Abu Hussein, 2021, p. 20).

3. dimensions of cybersecurity in tourism companies:

The dimensions of cybersecurity in tourism companies are as follows:

3/1 techniques:

Cybersecurity technologies include all modern

technological mechanisms and means used by individuals, bodies, and organizations in providing electronic protection to counter cyber threats and risks, including technologies for protecting computer devices, electronic networks, and smartphones by relying on what is known as firewall systems, and the application of computer antivirus software (Craigen, 2014, p.15) that provide procedures for the protection of personal data of individuals and corporate information to avoid opening unauthorized external links and make backup copies of information and data of interest (Mansour, 2021, p. 226).

Operations:
Cybersecurity operations are defined as operational security operations that include various activities and practices that deal with information files and important data assets of companies, ensuring their protection from cyber threats and providing timely access to them to authorized personnel only (Al-Jafari, 2021, p. 85), where the successful application of the successful cybersecurity concept begins from the first design stage of cybersecurity operations to ensure the maintenance of automated devices and information systems programs within the organization (Al-Samhan, 2020, p. 14).

Individuals:
This includes companies ' keenness to hire specialized and qualified personnel to deal with modern technical means related to the field of cybersecurity and the acquisition of human resources with competence in the implementation of electronic protection operations and management of technological technologies by the rules and standards of cybersecurity (Craigen, 2014, p.15).
Cyber technological challenges in tourism companies
Cyber challenges and attacks are defined by several terms, such as computer and Internet Crimes, Electronic Crimes, Information Crimes, and cybercrimes (said and Osmani, 2020, P.15). These terms refer to crimes committed by individuals, institutions or countries using electronic data storage operations, or various communication devices to seize, destroy, change, or use confidential data and information in illegal ways (Brown, 2015, p.57).
Among the most critical cyber challenges facing tourism companies are the following:

Computer viruses:
Computer viruses take several types and forms that destroy computer operating systems, disable them, damage their information stores, or stop the work of some physical parts in which computers are damaged (Farouk, 1999, p.7) through some electronic programs that are deliberately deployed, to change the characteristics and attributes of files recorded on the computer to destroy their information content (Khalifa, 2017, p. 82).

Ransomware:
These programs are electronic software (getaway programmers), where they encrypt the information content on the computer disk to extort the customer or company and demand a ransom of money to restore the encrypted information content. These programs rely on a built-in timer and by the payment deadline. In non-compliance with the payment date, the device becomes inaccessible to files or stored information. Despite the inability of these programs to encrypt shared drives, the subscriber is on the file server (Smith & Lustre, 2021, p. 4).

Electronic phishing:
It means a cyber deception operation that aims to defraud customers using personal data by sharing personal data, such as a password or credit card data (garden and al-Rabeei, 2020, P.188), as well as the possibility of cyber deception in electronic conflicts within cyberspace, which relies on the element of surprise and penetrates cyber security tools by various means such as disinformation, electronic jamming, and impersonation until it reaches the process of electronic blackmail (Hamza et al., 2021, p. 166).

4/4 electronic espionage:
It represents the most important and most famous types of cyber threats to which

companies and business organizations are exposed, as well as the risks of threatening the national security of countries, the most famous of which are eavesdropping operations carried out on information and data stored on computers, or confidential data recorded on websites or mobile phones (Hamza et al., 2021, p. 165).

Cyber hacking:

It represents the most significant and most dangerous cyber threats in cyberspace because it constitutes a comprehensive technical weapon through which it is possible to control computers fully, access all information and data stored on them, control them, and control the means of electronic communication, in personal computers and mobile phones. Those responsible for this cyber hacking are known as hackers (Giroud, 2013, p.111).

Cyber flies:

These fake accounts are created on social networking sites to launch biased and inciting media campaigns against individuals, companies, entities, and even countries, and maybe for political or propaganda purposes (Abadi, 2018, p. 10). They are in the form of a package of advertising media programs that display advertising materials during the operation of the software and include negative or extremist religious, moral, or political messages that threaten community peace (gaidan and al-Rabeei, 2020, P. 191) through the dissemination of false information, or misleading news, which has a negative propaganda effect on the intended destinations (Franz, 2011, p.4).

Cybersecurity requirements to meet technological challenges in tourism companies:

The ITU has developed the principles of the global cybersecurity program, which represents the Cybersecurity Index, which consists of five basic requirements: legal, technical, organizational structures, capacity-building, regional and international cooperation as follows:

5/1 legal requirements:

The issue published by the ITU in 2009 under the title (Manual for developing countries of essential measures in the field of cyber security) is an effective tool to help states and bodies apply approaches, evaluate cyber security operations and counter cyber threats at the national and international levels (itu, 2009), the ITU also issued in the same year the legislative toolkit on cybercrime, which provides member states with a model a convenient reference for legal and legislative formulations of assistance In the adaptation of laws and procedural regulations related to cybersecurity (itu, 2010, p. 41).

5/2 technical requirements:

Includes various measures and procedures adopted by technical organizations in dealing with cybersecurity threats (ITU, 2009).

5/3 regulatory requirements:

It includes all the measures and strategies adopted by organizations in order to coordinate policies towards framing cybersecurity systems at the national level, and in this context, the Iraqi government has established the cyber events response team under the supervision of the Iraqi national security advisor, this national team is specialized in securing the protection of national networks, data centers, and government sites, dealing with cyber incidents, providing protection for internet infrastructure, contributing to spreading awareness of the importance of protecting electronic privacy of individuals and institutions on the internet and supporting cybersecurity efforts in the public and private sectors (Khurasan, 2021, p.10).

Total index	Cooperation requirements	Capacity building requirements	Regulatory requirements	Technical requirements	Law requirement
20.05	4.6	2.14	7.75	6.56	0.00

Applied Framework

1. Field Study Methodology

Designing the questionnaire form
The questionnaire form was designed in the form of personal questions related to the demographic variables of the study sample, and objective questions related to the role of cybersecurity in facing technological challenges in tourism companies in the city of Baghdad, where one of the answers is selected in the questionnaire form, the questionnaire form consisted of (23) questions, the first section included demographic data and consisted of (3) questions, the second section included objective data, and consisted of (20) questions divided into three axes the first axis the role of technologies in achieving cybersecurity to meet technological challenges in tourism companies in the city of Baghdad and consisted of (7) questions, the second axis is the role of operations in achieving The third axis is the role of individuals in achieving cyber security to meet the technological challenges in tourism companies in the city of Baghdad and consist of (6) questions, and the third axis is the role of individuals in achieving cyber security to meet the technological challenges in tourism companies in the city of Baghdad and consist of (7) questions.

Scale of responses:
The responses were formulated on the fifth Likert Likert scale, and the scale scores were classified as follows Table (2):

Completely agree	agree	Natural	disagree	Completely disagree	Category
5	4	3	2	1	Score
Greater than 4.2 to 5.0	Greater than 3.4 to 4.2	Greater than 2.6 to 3.4	Greater than 1.8 to 2.6	From 1.0 to 1.8	Term

Table- 2 *(shows the scale of the answer to the questionnaire paragraphs)*

Tests of the truthfulness and constancy of the questionnaire:

The honesty of internal consistency was used to measure the honesty of the questionnaire scale, using the Pearson correlation coefficient between each paragraph of the questionnaire and the average response

.

Statistical Significance	Correlation Coefficient	Paragraphs		No.

The first axis - the role of technologies in achieving cybersecurity to meet technological challenges in tourism companies				
0.000	**0.645	The company has a specific electronic system that allows employees to access company devices using secure passwords		1
0.000	**0.663	The company has a security system that defines the responsibilities of each individual and allows access to information bases according to the specializations and powers granted		2
0.000	**0. Right	The company uses original global programs to protect devices from computer viruses		3
0.000	**0.563	The company has a security system to monitor and detect cyber-attacks and electronic hacking		4
0.000	**0.564	There is an electronic system to protect customer data within the company		5
0.000	**0.771	The company uses an electronic system to ensure the confidentiality of information exchange between employees within the company		6
0.000	**0.762	The company uses an electronic system to protect and exchange information via e-mail, fax, and websites		7
The second axis - the role of operations in achieving cybersecurity to meet technological challenges in tourism companies				
0.000	**0.703	The company is committed to the professional rules and procedures regulating cybersecurity work		8
0.000	**0.660	The company is committed to transparency regarding the risks of electronic hacks and cybersecurity threats		9
0.000	**0.545	There are planned work processes for the flow and circulation of data among the company's employees according to specializations and		10

		authorities		
0.000	**0.659	The company is conducting a continuous assessment of the weaknesses in its technical capabilities in the field of cybersecurity		11
0.000	**0.602	The company has contingency plans to deal with cyber threats		12
0.000	**0.791	The company considers cybersecurity as one of the elements of competitive advantage to enhance the brand and improve the company's reputation in the tourism market		13
The third axis - the role of individuals in achieving cybersecurity to meet technological challenges in tourism companies				
0.000	**0.847	The company has individuals specialized in the tasks of securing electronic data and implementing cybersecurity rules		14
0.000	**0.830	The company is keen to appoint specialists in the field of cybersecurity		15
0.000	**0.859	The company uses outside specialists to help build cybersecurity systems		16
0.000	**0.824	The company provides training courses to qualify its human resources in the field of cybersecurity		17
0.000	**0.558	The company encourages employees to innovate and be creative in the field of cybersecurity systems to save the expenses of relying on external cybersecurity systems		18
0.000	**0.644	The company helps workers follow the latest global systems in the field of cybersecurity		19
0.000	**0.588	The company provides financial and technical resources to develop the professional capabilities of its employees in the field of cybersecurity		20

Table- 3 *(validates internal consistency using (Pearson correlation) of questionnaire paragraphs.)*

It is clear from Table (3) that all Pearson correlation coefficients between each paragraph of the questionnaire and the average responses to the axis to which it belongs were statistically significant at the level of 0.01 in all paragraphs, and this indicates a high degree of internal consistency of the questionnaire paragraphs.

The Cronbach-Cronbach Alpha coefficient was used to test the stability of the scale for the questionnaire form in order to verify the degree of stability of the scale used, using the statistical program (SPSS, V.24).

Cronbach's Alpha Coefficient	Number of Paragraphs	Title	The Hub
0.650	7	The Role of Technologies in Achieving Cybersecurity to Meet Technological Challenges In Tourism Companies	The First
0.722	6	The Role of Operations in Achieving Cybersecurity to Meet Technological Challenges In Tourism Companies	The Second
0.766	7	The Role of Individuals in Achieving Cybersecurity to Meet Technological Challenges In Tourism Companies	The Third
0.750	**20**	**Total Questionnaire**	

Table -4 *(cronbach's Alpha constancy coefficient for the questionnaire axes.)*

It is clear from Table (4) that the alpha Cronbach coefficient for the questionnaire form consisting of 20 questions was 0.750, which indicates a high degree of stability of the questionnaire form's paragraphs.

1/4 determination of the study sample:

The random sample Method was used to determine the sample size of the study (110 individuals) of employees of tourism companies in Baghdad through the distribution of the electronic questionnaire on Google Forms.

1/5 statistical tools used:

Some statistical tools were used to analyze the questionnaire using the statistical analysis program SPSS, V.24: (percentage - arithmetic mean - standard deviation- Cronbach's Alpha coefficient - Pearson Pearson correlation relations - single Sample T test-simple linear regression).

2-descriptive statistics of the questionnaire form:

2/1 descriptive statistics of demographic data:

SMA	Percentage	Repetition	Response	Variable
1.3	66.4%	73	**Male**	**Gender**
	33.6%	37	**Female**	
2.1	21.8%	24	Less than 30 years old	**Age**
	58.2%	64	From 30 years to less than 40 years	
	18.2%	20	From 40 years to less than 50 years	
	1.8%	2	50 years and older	
2.2	24.5%	27	Less than 5 years	**Years of Experience**
	51.8%	57	From 5 to less than 10 years	
	18.2%	20	From 10 to less than 15 years	
	5.5%	6	More than 15 years	

Table-5 *(statistical analysis of demographic data for the study sample)*

Table (5) shows the demographic characteristics of the study sample in terms of gender; the number of males was 73 individuals by 66.4%, and the number of females was 37 individuals by 33.6%, with an arithmetic average of 1.3, and it turned out that the prevailing age group is from 30 to less than 40 years with several 64 individuals by 58.2% with an arithmetic average of 2.1, while the number of years of experience prevailing in the category of 5 to less than ten years was 57 individuals by 51.8%, with an arithmetic average of 2.2

2/2 descriptive statistics of objective data:

The first axis – the role of technologies in achieving cybersecurity to meet technological challenges in tourism companies:

Standard Deviation	SMA	Totally Agree	Agree	Neutral	Disagree	Completely Disagree	Repetition	Phrase
1.05	4.00	53	12	37	8	0	Repetition	The company has a specific electronic system that allows employees to access company devices using secure passwords
		48.2	10.9	33.6	7.3	0	%	

1.03	4.00	50	17	37	5	1	Repetition	The company has a security system that defines the responsibilities of each individual and allows access to information bases according to the specializations and powers granted
		45.5	15.5	33.6	4.5	0.9	%	
0.96	4.26	63	18	25	3	1	Repetition	The company uses original global programs to protect devices from computer viruses
		57.3	16.4	22.7	2.7	0.9	%	
0.92	4.17	55	22	30	3	0	Repetition	The company has a security system to monitor and detect cyber attacks and electronic hacking
		50.0	20.0	27.3	2.7	0	%	
1.00	4.05	53	15	37	5	0	Repetition	There is an electronic system to protect customer data within the company
		48.2	13.6	33.6	4.5	0	%	
0.96	4.12	56	15	36	3	0	Repetition	The company uses an electronic system to ensure the
		50.9	13.6	32.7	2.7	0	%	

								confidentiality of information exchange between employees within the company
1.02 standard deviation	4.20 SMA	63	13	27	7	0	Repetition	The company uses an electronic system to protect and exchange information via e-mail, fax, and websites
		57.3	11.8	24.5	6.4	0	%	

Table-6 *(statistical analysis of the opinions of the study sample on the role of technologies in achieving cybersecurity to meet technological challenges in tourism companies)*

Table (6) shows the opinions of the study sample on the role of technologies in achieving cybersecurity to meet technological challenges in tourism companies, as it turned out that most employees believe that the company has a specific electronic system that allows employees to enter the company's devices using secure passwords with an average account of 4.0, and that the company has a security system that determines the responsibilities of each individual and allows access to information databases according to specialties and powers granted with an average account of 4.0, and that the company uses original international programs to protect devices from computer viruses with an average account of 4.26, and they also believe that the company has a security for monitoring and detecting cyber-attacks and electronic penetration with an average account of 4.17, that there is an electronic system for protecting customer data within the company with an average account of 4.05, that the company uses an electronic system to ensure the confidentiality of information exchange between employees within the company with an average account of 4.12, and that the company uses an electronic system to protect information and Exchange it via e-mail, fax and websites with an average account of 4.20, and all the values of the standard deviation indicated the presence of dispersion in the opinions of the study sample.

The second axis – the role of operations in achieving cybersecurity to meet technological challenges in tourism companies:

Standard Deviation	SMA	Totally Agree	Agree	Neutral	Disagree	Completely Disagree	Repetition	Phrase
1.00	4.11	57	14	34	5	0	%	The company is committed to the professional rules and procedures
		51.8	12.7	30.9	4.5	0	Repetition	

								regulating cybersecurity work
1.11	3.95	52	13	34	10	1	%	The company is committed to transparency regarding the risks of electronic hacks and cybersecurity threats
		47.3	11.8	30.9	9.1	0.9	Repetition	
0.97	4.05	53	12	43	2	0	%	There are planned work processes for the flow and circulation of data among the company's employees according to specializations and authorities
		48.2	10.9	39.1	1.8	0	Repetition	
1.00	3.93	47	14	44	5	0	%	The company is conducting a continuous assessment of the weaknesses in its technical capabilities in the field of cybersecurity
		42.7	12.7	40.0	4.5	0	Repetition	
0.93	4.20	59	16	33	2	0	%	The company has contingency plans to deal with cyber threats
		53.6	14.5	30.0	1.8	0	Repetition	
1.03	4.03	53	16	33	8	0	%	The company

standard deviation	SMA	48.2	14.5	30.0	7.3	0	Repetition	considers cybersecurity as one of the elements of competitive advantage to enhance the brand and improve the company's reputation in the tourism market

Table -7 *(statistical analysis of the opinions of the study sample on the role of operations in achieving cybersecurity to meet technological challenges in tourism companies)*

Table (7) shows the opinions of the sample of the study on the processes in achieving cybersecurity to meet technological challenges in tourism companies, where it was found that the employees of tourism companies see the company's commitment to the rules and professional procedures governing the work of cybersecurity with an average account of 4.11, and the company is committed to transparency regarding the risks of electronic breaches and threats to cybersecurity with an average account of 3.95, and that there are planned courses of action for the flow and circulation of data among the company's employees according to the terms of reference and powers with an average account of 4.05, and that the company is conducting a continuous evaluation process for weaknesses in its technical capabilities in the field of cybersecurity with an arithmetic average of 3.93, he The company has contingency plans to deal with cyber threats with an average calculation of 4.20, and the company considers cyber security as one of the elements of competitive advantage to enhance the brand and improve the company's reputation in the tourist market with an average calculation of 4.03, and all the values of the standard deviation indicated the presence of dispersion in the opinions of the study sample.

The third axis – the role of individuals in achieving cybersecurity to meet technological challenges in tourism companies:

standard deviation	SMA	Totally agree	agree	neutral	disagree	Completely disagree	Repetition	Phrase
1.04	3.87	46	11	46	7	0	%	The company

		41.8	10.0	41.8	6.4	0	Repetition	has individuals specialized in the tasks of securing electronic data and implementing cybersecurity rules
1.01	4.03	54	10	42	4	0	%	The company is keen to hire specialists in the field of cybersecurity
		49.1	9.1	38.2	3.6	0	Repetition	
1.03	3.93	50	8	47	5	0	%	The company uses outside specialists to help build cybersecurity systems
		45.5	7.3	42.7	4.5	0	Repetition	
1.07	3.89	47	13	43	5	2	%	The company provides training courses to qualify its human resources in the field of cybersecurity
		42.7	11.8	39.1	4.5	1.8	Repetition	
0.99	4.11	55	19	30	6	0	%	The company encourages employees to innovate and be creative in the field of cybersecurity systems to save the expenses of
		50.0	17.3	27.3	5.5	0	Repetition	

								relying on external cybersecurity systems
0.83	4.40	66	25	16	3	0	%	The company helps workers follow the latest global systems in the field of cybersecurity
		60.0	22.7	14.5	2.7	0	Repetition	
0.83 standard deviation	4.37 SMA	62	30	16	1	1	%	The company provides financial and technical resources to develop the professional capabilities of its employees in the field of cybersecurity Phrase
		56.4	27.3	14.5	0.9	0.9	Repetition	

Table-8 *(Statistical analysis of the opinions of the study sample on the role of individuals in achieving cybersecurity to meet technological challenges in tourism companies)*

Table (8) shows the opinions of the study sample on the role of individuals in achieving cybersecurity to meet technological challenges in tourism companies, as it turned out that the company has individuals specialized in the tasks of securing electronic data and applying cybersecurity rules with an average account of 3.87, the company is also keen to appoint specialists in the field of cybersecurity with an average account of 4.03, and they believe that the company uses specialists from abroad to help build cybersecurity systems with an average account of 3.93, and that the company provides training courses to qualify its human resources in the field of cybersecurity with an average account of 3.89, the company encourages employees to innovate and be creative in the field of security systems The company helps employees to follow the latest international systems in the field of cybersecurity with an average calculation of 4.11, and the company also provides financial and technical resources to develop the professional capabilities of its employees in the field of cybersecurity with an average calculation of 4.37, and all the values of the standard deviation indicated the presence of dispersion in the opinions of the study sample.

3 - Testing the validity of the assumptions:

3/1 testing the first hypothesis:

The validity of the first hypothesis was tested using the Test (t-test) for one sample at a morale level (0.05) using the SPSS program as follows:

Probability of Significance P	Confidence 95 Interval for The Difference Between the Means		T-Test	Standard Error of The Mean	Standard Deviation	Average
	The Highest Rate	Minimum				
0.000	4.40	3.65	50.9	0.052	0.87	4.1

Table -9 *(Test (t-test) of the hypothesis of the first study)*

It is clear from Table (9) that the probability of significance p is smaller than the moral level (0.05), and therefore the nihilistic hypothesis is rejected, and the alternative hypothesis is accepted.there are significant moral differences between the opinions of the study sample about the role of cybersecurity in facing technological challenges in tourism companies in the city of Baghdad.

3/2 testing the second hypothesis:

The validity of the second hypothesis was tested using a simple linear regression test at a significant level (0.05) using the SPSS program, 24 as follows:

Significance Level	Indicative Value	T-Test Value	Standard Error	Estimated Value	Landmarks
0.05	0.000	20.225	0.112	0.560	Fixed part (facing technological challenges in tourism companies)
0.05	0.000	32.605	0.120	0.150	1 – Cybersecurity
0.606	R	The value of the correlation between variables			
0.660	R2	The coefficient of determination			
0.039	Adj.R2	Modified coefficient of determination			
720.00	F	Test value (P)			
0.000	P-Value	The significance value of choosing (F)			

Table-10 *(results of a simple regression analysis of the impact of cybersecurity in the face of technological challenges in tourism companies.)*

From the analysis of Table (10), it is clear that there is a strong direct relationship between cybersecurity and facing technological challenges in tourism companies, where the

correlation coefficient (R) reached (0.606); the value of interpretability of the regression model represented by the coefficient of determination (R2) also reached (0.660); indicating that 66% of the changes in the face of technological challenges in tourism companies are explained by cybersecurity, and the value of (F) calculated in the regression model reached 720.00 (Sig= 0.000), which is smaller than the approved statistical significance level (0.05), and this indicates the presence of a statistically significant moral impact of cybersecurity in the face of technological challenges in tourism companies ،This indicates the rejection of the nihilistic hypothesis, and the acceptance of the alternative hypothesis that " there is a statistically significant impact of cybersecurity on meeting the technological challenges of tourism companies in the city of Baghdad ".

CONCLUSION

Cybersecurity refers to the security field related to protecting digital information systems, networks, and websites connected to the internet, monitoring threats through cyberspace, dealing with and preventing them, and countering their effects on individuals and public and private institutions.

The importance of cybersecurity has recently increased in light of the widespread use of the internet, the growing dependence of tourism companies on digital technology, and the increasing pace of electronic business, which requires activating cybersecurity to protect the company's data and its customers.

The dimensions of cybersecurity in tourism companies include three areas: technologies (cyber technological means), operations (cyber organizational means), and personnel (cyber human resources).

The most critical cyber challenges facing tourism companies are computer viruses, ransomware, phishing, electronic espionage, cyber piracy, and cyber flies, which are the most famous types of cyber threats

The Cybersecurity Index, within the framework of the principles of the global cybersecurity program, consists of five basic requirements: legal, technical, organizational structures, capacity-building, regional and international cooperation

The Iraqi national security advisor has established a Cyber Incident Response Team to take responsibility for protecting national networks, data centers, and government sites, responding to cyber threats, and spreading awareness in the field of cybersecurity

Iraq's ranking in the Global Cybersecurity Index declined from position (107) globally and (13) Arabs in 2018 to the position (129) globally and (17) Arabs in 2020, reflecting the increasing volume of cyber threats and associated technological challenges, which is reflected in the work of Iraqi tourism companies

Tourism companies provide the necessary technologies and mechanisms to achieve cyber security, meet technological challenges, secure their corporate and customer data, and provide protection from computer viruses

Tourism companies take professional measures to ensure the application of cybersecurity rules and deal with cyber technological threats as a competitive advantage and an operational necessity

Tourism companies seek to develop the capabilities of individuals and qualify human resources to achieve cybersecurity by using specialized expertise and providing financial and technical support to meet technological challenges

The results of the first hypothesis test showed that there are significant moral differences between the opinions of the study sample on the role of cybersecurity in facing technological challenges in tourism companies in Baghdad

The results of the second hypothesis test showed that there is a statistically significant impact of cybersecurity on meeting the technological challenges of tourism companies in the city of Baghdad

Recommendations:

Legislating the cybersecurity law that criminalizes illegal cyber businesses and establishing the necessary controls and rules to regulate and protect cyber businesses.

Activating the role of the cyber events response team in Iraq in carrying out its responsibilities in

addressing cyber technological threats and supervising the information security sector in public and private institutions, especially the business sector based on electronic commerce, such as tourism companies.

Establishment of a unique Information Security Department in tourism companies to provide security protection of information and institutional data and maintain the confidentiality of customer and employee data.

Allocate financial, technical, and professional resources to support cybersecurity efforts in tourism companies as an essential element to achieve competitive advantage and improve their reputation.

Use specialized experts in cyber security and take advantage of leading international experiences to provide cyber security in tourism companies.

Providing training and qualification for human resources in tourism companies to deal with cyber technological threats and activate cybersecurity programs and applications

Developing a comprehensive and integrated cybersecurity strategy within the framework of international rules and standards and the principles of the global cybersecurity program to improve Iraq's position in the Global Cybersecurity Index.

REFERENCES

1. Abu Hussein, Haneen Jamil (2021): The legal framework for cybersecurity services comparative study, master's thesis, Faculty of Law, Middle East University, Jordan.
2. Al-Abadi, Islam Issa (2018): Cyber terrorism, its dangers, characteristics and objectives of combating it, House of Thought and Law, Amman.
3. Al-Adalah, Abdulrahman Akram Abdulrahman (2021): Enhancing cybersecurity within the country and its role in maintaining national security fifth generation of weapons field study in Jordan 2012-2021, master thesis, Bayt al-Hikma Institute, Al-Bayt University, Jordan.
4. Al-January, Khaled Makhlef (2021): Digital transformation of national institutions and cybersecurity challenges from the point of view of academic police officers in Kuwait, the Arab Journal of Arts and Humanities, the Arab Foundation for Education, Science, and Literature, Vol.5, No. 19.
5. Al-jumps, Gohar (2016): The assumption and revolution of the place of the Internet in the emergence of Arab civil society, the Arab Center for Research and Policy Studies, Beirut.
6. Al-Khudari, Jihan Saad Mohammed, salami, Hoda Jibril Ali, and kalibi, Naama Nasser madbash (2020): cybersecurity and artificial intelligence in Saudi universities A Comparative Study, Journal of university performance development, Mansoura University, Vol.12, No. 1.
7. Al-Samhan, Mona Abdullah (2020): Requirements for achieving cybersecurity for administrative information systems at King Saud University, Journal of the Faculty of Education, Mansoura University, No. 111.
8. Amoroso, E. (2007): Cybersecurity, Silicon press
9. Atiya, Idris, (2019): The place of cyber security in the Algerian national security system, Vol.1, No. 1.
10. Basri, Nasir Abdul Razzaq, Hassan, Nour Mansour (2021). Innovative City Applications and their Role in Supporting Religious Tourism, Al-Sabat magazine, Karbala Center for Studies and Research, Iraq, Vol. 7, No. 2
11. Belford, Lotfi LeMine (2016): Cyberspace engineering and actors, Algerian Journal of Political Studies, No. 5.
12. Brown, C. S. (2015): Investigation and prosecution of cybercrime: Forensic dependencies and barriers to justice, International Journal of Cybercrime, Vol. 9, Issue 1
13. Chalabi, Ali Abdel Razek, and Ahmed, Hany Khamis (2009): Globalization and everyday life, Anglo-Egyptian Library, Cairo.

14. Craigen, d, Deacon Tebow, N, and Purse, R. (2014): Defining cybersecurity, technology innovation management review (Ottawa: Technology Innovation Management Review, October 2014.
15. Farouk, Hussein (1999): Computer viruses, Arab printing and publishing house, Cairo.
16. Franz, T. V. (2011): Professional realization of electronic warfare for the development of the next generation.
17. Ghadban, Rabi'i, Mohamed Munther (2020): Cybersecurity and the politics of international confrontation, Journal of Strategic and Reverse Studies, Arab Democratic Center, Vol.2, No. 9, Berlin.
18. Giloud, Walid Ghassan said (2013): The role of electronic warfare in the Arab-Israeli conflict, master thesis, Faculty of graduate studies, Nablus University.
19. Hamza, Ahmed, and Al-Bar, Amin, and Mo'min, emotions (2021): The Implications of Cyber Threats on the Security of Society, in the book Environmental Governance, Environmental Governance and the Challenges of Sustainable Development, A Comparative Study between Economics and international environmental law, Arab Democratic Center, Berlin.
20. International Telecommunication Union (ITU) (2009): Security in Communications and Information Technology Handbook for developing countries, Geneva.
21. International Telecommunication Union (ITU) (2010): Plan of action C5 of the World Summit on the Information Society, Geneva.
22. Kadaifa, Amina (2016): Information Security Strategy, Economic Dimensions magazine, almaged6.
23. Khalifa, Ihab (2017): Electronic Power: How countries can manage their affairs in the Internet age, Dar Al-Arabi Publishing and Distribution, Cairo.
24. Khurisan, Basem Ali (2021): Cybersecurity in Iraq, a reading in the Global Cybersecurity Index 2020, Al Bayan Center for Studies and Planning, Baghdad.
25. Lakhal, a life, and Lakhal, Muhammad, and Ibn Aada Um Muhammad (2022). ICT is a modern approach to activating governance in business organizations, Journal of Social Responsibility and Sustainable Development, Algeria, Vol. 4, No. 1
26. Machouche, Mourad (2018): International efforts to combat cybercrime, Faculty of Legal, economic and Social Sciences, Hassan I University, Morocco
27. Mansour, Amna Mohammed (2021): The impact of cybersecurity on internal control and the economic unit a survey study, Journal of Management and Economics, Mustansiriya University, No. 127.
28. NATO, North Atlantic Treaty Organization, (2016): Cybersecurity general reference curriculum, Brussels
29. Said, Khaled, and Osmani, Abdul Rahman (2020): The conceptual framework of cybercrime, in the book Cybercrime and its Impact on Economic Development, Arab Democratic Center, Berlin.
30. Smith, Zhanna Malkus, luster, Eugenia (2021): The hidden costs of cybercrime, Al Bayan Center for Studies and Planning Studies series, Baghdad.