REQUIREMENTS TO SUPPORT A MANAGEMENT INFORMATION SYSTEM TO CONFRONT THE CYBER THREAT IN THE IRAQI TRADE BANK.

ASST. PROF SALMAN ABOOD ZBAR

Technical institute of Al-Mussaib, AL- Furat AL-Awsat Technical university (ATU), 51009, Iraq
Email: lnm.slm@aut.edu.iq

Abstract
The study aims to use the requirements of cybersecurity approved by the World Economic Forum and the suggestions added by the researcher to support the decision to develop or establish a management information system in the Iraqi Trade Bank, Using the multi-characteristic utility theor. The study reached that the use of decision support models to reject the current system or develop it for its inability to confront the cyber threat and choose the best alternative (creating a new system). The research recommended the implementation of the cybersecurity strategy in Iraq, including the Iraqi Trade Bank, where the index measuring the implementation of global cyber risk standards showed a significant decline of 129 globally.

Key Words: decisionsupport, cyberattacks, best alternative, requirement, management information system.

INTRODUCTION

One of the most important areas of cyber transformation in the year 2022, and before it, was the realization by many countries and institutions that cyber capabilities have become an important field for exercising influence and achieving superiority and competition, as arsenals of conventional weapons are no longer the main criterion for measuring the overall strength of a state, after the Fourth Industrial Revolution. And the accompanying manifestations of artificial intelligence. In this context, many countries have developed national policies and strategies to keep pace with the leaps of development in the Fourth Industrial Revolution, especially after the escalation of international conflicts in cyberspace, which have become an integral part of international interactions with the remarkable increase in rates of cyberattacks and risks.

As a corollary of this international cyber scramble, the global defense cyber security market was valued at $16.22 billion in 2020,and is expected to reach $28.53 billion by 2026 ,registering a compound annual growth rate of approximately 10.51% during the forecast period (2021-2026) . **(1,2)** It is expected that the size of the cybersecurity market in the Middle East will grow at a compound annual growth rate of 17.1 , from $20.3 billion in 2022 to $44.7 billion in 2027. **(3)**

A certain mechanism must be found to protect the system from cyber intrusion Considering the decision support system as one of the systems that affect the determination of the alternatives available to the decision-maker to choose the best of them, which can be defined (Provide managers with tools, not information, to help to help them solve structural and non-structural problems. the areas of their use and application have expanded, which necessitated the need to develop them with the development of information technology) . **(4)** This model determines the correct sound decision through his experience and personal wisdom to support a specific requirement that it is more important than other requirements that Limited by the World Economic Forum **(5)**(**Building cyber resilience , Enhancing global cooperation , Understanding Future Networks andTechnology ,Cybersecurity awareness , Cybersecurity governance and risk management , Developing new rules and legislation , International Cooperation) .**

The researcher added to it a proposed requirement (**returning to traditional technology, merging between more than one requirement , and cyber risk insurance**) to complete the picture in front of the decision-maker and that experience and personal judgment are not sufficient to produce a sound decision, but the use of technical methods in designing a decision support system to produce accurate results, where mathematical models are formed for the problem and through these models and their solutions and the analysis of their results, a group of alternatives is evaluated for

the decision-maker so that each alternative occupies a specific decision, and is considered the multi-characteristic utility theory is highly compatible with choosing the best alternative for developing or establishing a new management information system that supports the decision-making process **.**

THE FIRST TOPIC: STUDY METHODOLOGY
FIRST:STUDYPROBLEM

The penetration of information systems, network systems and information sites has affected many organizations in recent years and with the passage of time we find that despite the means of protection that organizations follow, there is a clear correlation in the rate of penetration with the variety of means used in Penetration as for the last sale that information systems can face, it is a threat, some of which may be associated with theft of information or the entry of viruses and others, which are more harmful to information systems, and it may sometimes be terrifying to predict the hostile motives of the people who carry them out.   .

Therefore, the decision maker to confront cyber threats may not be available , What are the methods, procedures and alternatives that can be used to reduce the damage, and   evaluate the best alternatives, so the research problem can be summed up with the following questions:

1.What are the characteristics or requirements available to the decision-maker to confront   cyber threats?

 2.Developing or establishing an information system compatible with the requirements or characteristics of cyber security .

3.Evaluate the available alternatives according to the benefit to the decision-maker in the surveyed banks .

 Second: Study Objectives : This research aims to develop proposed requirements or descriptions for managing and confronting the cyber risk in accordance with the World Economic Forum and what the researcher presented in terms of adding requirements that allow the decision-maker to choose more than one alternative according to the conditions surrounding the banks under study and the extent of their contribution to reducing the damages resulting from those risks.

Third: Study importance: It is considered a contribution to changing the patterns available to the decision-maker and defining them in light of the ISO standards, but adding requirements or descriptions that may achieve effectiveness in making the right decision when using decision support models and choosing the best alternatives .   **Fourth :Hypotheses of study :**The study aims to achieve the following assumptions: **The first hypothesis**: The relative importance of the requirements of the management information system of the Trade Bank of Iraq for the cyber threat is not equal .   **The second hypothesis**: Choosing the best alternative to develop or establish an management information system in the Trade Bank of Iraq to confront the cyber threat depends on the benefit achieved.

 FifthResearch methodology : The research relies on the inductive approach to   identify the concept of decision support in determining alternatives, as well as deducing the most important cyber risk requirements approved by the World Economic Forum and research proposals by adding requirements that may contribute to choosing the development or construction of an information system that enables the decision-maker to determine priorities and possibilities to counter the cyber risk .

 Sixth : Research limits: The research was applied in Iraqi Trade Bank that deal with electronic commerce and digital transfer, and practical data were taken, which the research only applied to apply the multi-characteristic utility to extract decision support models.

The secound Topic : The research consists of two requirements : The first requirement is concerned with decision support systems, while the second requirement is concerned with cybersecurity :

 1/2Concept of Decision Support System (DSS) : There are many definitions of Decision Support System (DSS), it has been defined as " where tools can be provided computerized processing to

help clients, managers, and managers organize and analyze data for decision-making" . **(6)** and **(7)** defined decision support systems as the use of human resources with computer systems to improve the quality of decision, which is Computer-based systems to support decision-makers who deal with unstructured andsemi-structured problems.

2/2 Characteristics of decision support systems :Decision support systems are characterized by a set of characteristics that work to support decision makers, as follows: **(8) ,(9)**

-Providing data and forms necessary to solve problems and make structural, semi-structural and non-structural decisions, and thus provides support to all administrative levels, especially senior management.

-Focusing on the quality and effectiveness of the decision-making process, not its efficiency.

- Focusing on interaction and flexibility in information and the ability to adapt to the requirements of the decision-maker and to quickly adapt to his needs and to any changes that occur in the internal environment.

- A tremendous ability to quickly interact with decision makers.

-The ability to model and contain different models and the ability to manage them. It provides support to the decision-maker, but does not replace him. The decision-maker maintains the control and oversight function over the decision-making process .   -Supporting all categories of decision makers according to their background.

- It has tremendous energy to choose and test a number of alternative policies.

-In addition to carrying a large volume of data.

- Working on integrating models and traditional methods in order to access data .   3/2

Objectives of Decision Support Systems: Decision support systems are designed to deal with solving problems of both semi-structural and non-structural types by separating the places and parts of the problem to help managers use their expertise and judgment in solving it through its basic components. Decision support systems aim at the following: **(10) (11)**

-Supporting managers' decisions, not changing them.

–Discover the potential behavior and actions to solve the problems. -Arranging specific solutions and providing a list of variable options that can be   implemented

-Assisting managers in making decisions to solve semi-structural problems.   -Improving the effectiveness of decision-making (accuracy, time and quality) and   not just its efficiency.

- Expanding the perception and ability of the decision-maker, not directly imposing solutions.

4/2Risks Facing Decision Support Systems: Managers have recently faced, with the large size and complexity of organizations, many difficulties in making decisions, which are represented in: **(12)**

- Error in making a decision that is far from achievement, to meet challenges, it is possible to make very quick decisions.

- The new tools and ideas resulted in a number of diverse solutions that are not free from trouble in choosing the best one .

- The task of extracting valuable information has become difficult because the data available at the present time are much compared to what it was before.

 - Customer safety has become the latest trend even in emerging countries.

- Also, government borders and policies cause disturbance to the company's trends. International positions in decision-making also play an important role.

- New materials and technology make tried and tested processes obsolete.

 The second requirement is concerned with cybersecurity :

 First:Cybersecurity: It is defined as "a set of technical and administrative procedures that include the processes and mechanisms applied by organizations to secure their digital infrastructure and maintain the confidentiality of data and information"**(13)   The researcher finds it difficult to define a comprehensive definition of cybersecurit**y as it changes Organizes and collects all the resources, processes and structures used to protect cyberspace and the systems that support cyberspace from events.

Terminology related to cybersecurity: We mention them: **(14)**

1. Cyberspace: It is a digital interactive environment that constitutes physical elements consisting of digital devices, network systems, software, and users, whether operators or users. It is called (the fourth arm of modern armies)

2. Cyber deterrence: It is defined as preventing harmful acts against national assets in the digital space and the assets that support digital operations

3. A cyberattack: is a harmful and deliberate attempt by individuals or institutions to penetrate the information system of other individuals or institutions, the aim of which is the desire to collect information, seize it, trade in it, prove superiority over the development of technical means, harm persons or entities, achieve profits and material gains, or threaten security. national and military.

Secound : Iraqi Cyber Security Strategy   (15)

 In the last decade, Iraq has taken a set of measures related to cybersecurity, which included radically developing electronic governance systems, facilitating transactions for the citizen, and protecting the individual, society, and institutions from cyber-events.

1.The work of Iraqi e-governance (2012-2015), as well as the document "The Government Interface Framework and the Architectural Design of the National Institution".

2. In the fall of 2012, Iraq launched the "National Policy for Communication and Information Security", in which it clarified a number of basic concepts of communications security policies.

3.The Technical Committee for Communications and Information Security was formed by the National Security Council in 2015 for the purpose of managing   Iraqi cybersecurity in its various aspects and levels

4.The team was established the Iraqi CERT National Response to Cyber Events in 2017, which consisted of four teams of specialists in the field of technology. I come from various related government institutions. The Iraq CERT Team is a trusted authority that enhances Iraq's ability to respond to cybersecurity incidents   **Third:Global Cybersecurity Index:(16)** The United Nations, through the International Telecommunication Union, established one of the United Nations specialized agencies responsible for matters related to communications and information technology, the "Global Cybersecurity Index", which is a composite and effective index. To measure the extent of countries' commitment to cybersecurity aimed at protecting (information and property from theft, corruption, or natural disasters, and allowing information and property to remain productive and accessible to its target users. The index collects 25 criteria in one measure to monitor the commitment of 193 ITU member states to cybersecurity throug following five pillars:

Table1:Paragraphs related to the index (GCI) of Iraq's position in cybersecurity.

Legal	Technical	Regulatory	Capacity building	Cooperation	Total
0.000	6.56	7.75	2.14	4.6	20.7

The index uses data collected from countries and sets questions to assess compliance, Through consultation with a group of experts, the questions are weighted in order to obtain the total points of the cybersecurity index (for any country). The Global Cybersecurity Index and its report has been issued since 2015. The index and report presents the efficiency of countries in the world in cybersecurity and makes comparisons between them. In the 2021 edition issued by the International Telecommunication Union, America came in first place with a score of 100% ,Saudi Arabia in second place with a score of 99.5%.and Iraq was ranked 129 globally and 17 among Arabs.**(17)**

Fourth:Requirements to face escalating threats : The World Economic Forum has identified the following   priorities   to   confront   the   growing   cyber   threats:.**(18)**

1. Building cyber resilience: Cyber resilience means the ability of a system to recover from shock in an optimal way, either by returning to its original state or to a new modified state. Cyber resilience assumes that minor or even major disruptions are inevitable, and that absolute security cannot be obtained. Cyber resilience can be considered as a "Plan B" in case something goes wrong **(19)** . Cyber resilience can be enhanced by developing and framing future solutions, and promoting effective practices across digital systems. In fact, there is an urgent need to work on developing information systems security programs, and to enhance their resilience in the face of cyber threats. It should be noted here that there is a growing segment of cybersecurity services companies, Including investigations to determine the source of cyber attacks. The maturity of cybersecurity firms, the development of advanced attribution methods, and the increasing complexity of an interconnected world reflect the growing scope, threat, and potential harm caused by cyberincidents. In this context, it is possible to benefit from such companies in strengthening information systems, not only in order to enjoy great resilience capabilities, but also to technically confront cyber threats**(20)** .   .

2.Enhancing global cooperation: In the sense of increasing global cooperation between stakeholders from the public and private sectors, by strengthening the collective response to cybercrime, and jointly addressing major security challenges.

3.Understanding Future Networks and Technology: Identify future cybersecurity opportunities and challenges related to Fourth Industrial Revolution technologies, and design solutions that help build trust. **(21)**

 4.Cybersecurity awareness: With the spread of cyber threats on a large scale, countries must invest in training programs and educate citizens and workers in institutions about protecting sensitive data in order to prevent unwanted access to systems and networks. It is important to advise users of the metaverse world to remain cautious and aware of what they are doing in this world, and to deal with platforms that seriously work to protect their users

5.Cybersecurity governance and risk management: including identifying threats to the country/organisation, and maintaining an inventory of all ICS assets, including hardware, software, and supporting infrastructure technologies. Hence, moving on to developing cyber security policies, procedures, trainings and educational materials applicable to industrial control systems, and developing and practicing incident response procedures that integrate IT and OT operations. .

6.Developing new rules and legislation: The increasing growth in attacks and threats in cyberspace requires the continuation of developing new regulations and legislation to achieve cybersecurity requirements, and to keep pace with these rapid developments in the field of cybersecurity threats

7.International Cooperation: In theory, an effective cyber deterrence would require a broad scheme of defensive and offensive cyber capabilities, backed by astrong international legal framework, as well as the ability to attribute an attack to an attacker beyond reasonable doubt. Designing defensive cyber capabilities and designing best legal tools is relatively uncontested. Many international organizations and bodies have taken steps to raise awareness, establish international partnerships, and agree on common rules and practices. One of the main issues of legal coordination is to facilitate the prosecution of perpetrators of cybercrime.The avenues available for arms control in this field are primarily information-sharing and standards-building, while structural approaches and attempts to completely ban electronic warfare means or restrict their availability are largely impossible due to the ubiquitousness and dual uses of information technology **(22)** . The human element is still considered the weakest link in this field, as research revealed that 88% of security breaches occur as a result of human errors.**(23)** .

8.Integration of more than one Requirement: In the sense that the decision-maker supports more than one characteristic by giving it more importance so that he can deal with cyber breaches, he supports the quality of international cooperation and the quality of insurance on cyber penetration of insurance companies and so on.   .

9.Back to traditional technology: It wore a return to traditional technology, but it is the use of the globally connected wide network within specific times in which the organization is fully alert and prepared to face the cyber threat, and reflect at other times using the internal network or the highest local level .

10. Cyber risk insurance : Currently, there are significant barriers to widespread use of cybersecurity to transform cybersecurity practices in the private sector. Although McAfee has indicated that the global economy suffers more than $1 trillion in annual losses due to cyberattacks, the entire cyber insurance market only collects $5.5 billion in annual premiums, according to Christian Momenthaler, CEO of the reinsurance firm. Zurich-based giant Swiss Re, as well as faltering growth in the cyber insurance sector. In that context, a survey conducted by the insurance company Resilience [in cyberspace] found that 77 percent of companies wanted to benefit from more cyber insurance coverage than they could obtain.**(24)**

In contrast, many insurance companies have been reluctant to expand coverage due to their lack of robust data access, modeling, and insurance process management tools that show how to diversify investment in order to mitigate risk. The problem is treating cyber risks as a unified threat. In fact, cyber risks include different types of threats .**(25)** Some cyber insurers have begun modeling and pricing different threats or particular forms of risk. It can then diversify the types of insurance it offers to limit losses. For example, insurance companies discovered that most of the vulnerabilities in the operating system affect only one operating system by it self. Therefore, insurance companies can reduce potential losses by offering coverage to some companies that use "Apple" devices, and to other companies that use "Windows" devices. With this risk-based approach, insurers can wisely increase their exposure to cyber risks, and help increase market size with electronic catastrophe bonds, much as the insurance industry did for hurricanes.

THE THIRD TOPIC : An applied study to establish or develop an information system IN THE IRAQI TRADE BANK TO COUNTER THE CYBER THREAT

 The study was applied in the Iraqi Trade Bank, which is one of the banks that deals electronically in financing and e-commerce operations, and which wants to develop and establish a management information system to confront the cyber threat. They'sBanks management has conducted a set of studies , I came to the conclusion that there is an offer to develop and another to establish a new system, and there has been opposition from some members of the Board of Directors to the policy of development and construction and they see that the current system is good and meets the requirements of the bank at the present time, so the Board of Directors decided to study the current situation with the offers presented by the researcher.   .

1/3 Studying the submitted offers: A committee was formed to study the submitted offers to determine the priorities of the requirements or characteristics that are consistent with choosing to develop or establish a new information system to confront the cyber threat. The committee has been Based on the recommendation of the committee formed in connection with the development or establishment of an information system, the proposals have been studied in the light of the previous requirements   .

Table(2) show Offer development or to create a new information system**(Assesment**)

Iteam	Requirements	Current	Development	Construction
1.	Building cyberr esilience	10 %	70%	60%
2.	Enhancing global cooperation	5%	80%	80%
3.	Understanding Future Networks andTechnology	40%	60%	80%
4.	Cybersecurity awareness	60%	90%	60%
5.	Cybersecurity governance and riskmanagement	30%	80%	95%
6.	Developing new rules and legislation	0	20%	20%
7.	International Cooperation	5%	90%	80%
8.	Integration of more thanone characteristic	0	60%	70%
9.	Back to traditional technology	0	10%	0
10.	Cyber risk insurance	0	40%	60%

 And since the current situation (the Bank information system) is not consistent with the cyber threat, **so the current situation is rejected**, meaning that the comparison will be between two offers, and the best of them will be selected using the multi-characteristic utility theory away from the method that the bank followed in its own study and it was a manual method, Assuming that development or construction .

2/3 Determining the relative importance of the requirements and descriptions of the offers: A questionnaire list was used that includes a set of questions to obtain a field guide the table shows the extent of satisfaction with the requirements for choosing a management information system,Table(3) show a society and a research sample who have experience in information technology.

Research community	Number of Questionnaire	number of valid responses	number of excluded responses	Rate of responses	percentage of sample representation
Information technology worker	23	16	6	73%	33%
Teachers in universities	15	15	-	100%	31%
Beneficiaries of the system in the	11	10	1	91%	2 1%

Bank					
Total	48	41	7		85%

Table(4) shows the weighted weight of each requirement by multiplying the priority multiplier by the relative weight and as follows:

Item	requirement	priority	priority value	multiple order ,value	weigh t	relative weight *10	weighted weight
1.	Building cyber resilience	6	1	2	4	(10*4/9) =4.4	8.88
2.	Enhancing global cooperation	2	5	10	2	(10*2/5) =4	40
3.	Understanding Future Networks and Technology	3	5	10	2	(10*3/5) =6	60
4.	Cybersecurity awareness	3	4	8	1	(10*1/5) =2	16
5.	Cybersecurity governance and risk management	3	4	8	4	(10*4/5) =8	64
6.	Developing new rules and legislation	4	3	6	2	(10*2/5) =4	24
7.	International Cooperation	1	6	12	-	(!0)=10	120
8.	Integrationmore characteristic	4	3	6	3	(10*3/5) =6	36
9.	Back to traditional technology	5	2	4	-	(10)=10	40
10.	Cyber risk insurance	6	1	2	5	(10*5/9) =5.55	11.1

Tota l						420

From what is noted in the above table, the priority is considered more important than the priority that follows it, so it is arranged in reverse of its priority, that is, the characteristic whose sequence (6) is the highest takes (1), and the characteristic whose sequence (5) takes (2) and which was evaluated by Search in the questionnaire list, and so on for the rest of the traits.

As for the relative weights, we find that the seventh criterion has priority alone, while the second priority is shared by requirement (2) andrequirement ((3, but with ratio of 2:3, respectively.The third priority is shared by the trait (4) and (5) but in a ratio of 1:4, and the fourth priority is shared by the trait (6) and (8) but with ratio of 2:3 and the fifth priority is the trait (9) alone, and the sixth priority has the trait (1)) and (10), but with ratio of 4:5 And in the event that there is a priority for more than one characteristic, the relative weight is distributed by adding the weight for both characteristics, . 2:3 combines equal 5, 1:4: combines, so it equals 5, and 4:5 combines, and it equals 9, and so on..This means**(accepting the first hypothesis that the relative importance of the decision maker's support requirements is not equal)**

Table(5) showsthe possibility of priority weighted by relative importance can be determined on this basis as follows:

$\qquad$ **possibility**

1.Building cyber resilience $\qquad$ (8,88/420)*100 =2,1

2.Enhancing global cooperation $\qquad$ (40 /420)*100= 9.5

3.Understanding Future Networks and Technology $\qquad$ (60/420)*100 = 14.2

4.Cybersecurity awareness $\qquad$ (16/420)*100 = 3.8

5.Cybersecurity governance and risk management $\qquad$ (64/420)*100 =15.2

6.Developing new rules and legislation $\qquad$ (24/420)*100 = 5.7

7.International Cooperation $\qquad$ (120/ 429)*100= 28.5

8.Integration of more than one characteristic $\qquad$ (36/420) *100= 8.5

9.Back to traditional technology $\qquad$ (40/420)*100 = 9.5

10.Cyber risk insurance $\qquad$ (11.1 /420)*100 = 2.64

 Total $\qquad$ = 100

3/3Choosing the best alternative using the multi-characteristics **utility theory**: After determining the relative importance of the attribute, the values of the attributes and their degree can be indicated for the offers (development and construction), then mark(*)for the best value of the attribute within the boundaries of the offers table, as well as put a line under the lowest value of the attribute within the offers : Table (6) shows the following:

Iteam	requirement	Possibility %	Development	Construction
1.	Building cyber resilience	2.11	80*	70
2.	Enhancing global cooperation	9.5	80	85*
3.	Understanding Future Networks and Technology	14.2	60	80*
4.	Cybersecurity awareness	3.8	90*	60
5.	Cybersecurity governance and risk management	15.2	80	95*
6.	Developing new rules and legislation	5.8	20	20
7.	International Cooperation	28.5	70	80*
8.	Integration of more than one characteristic	8.5	70*	60
9.	Back to traditional technology	9.5	10	0* best lowest
10	Cyber risk insurance	2.6	40	60*
Total		100		

Through the table (6) and after determining the relative weight of therequirement   , all the minimum and maximum values can be calculated, where all the numbers above it (*) are given a value of (1) and a value of (zero) is given for the minimum columns, and the minimum values can be symbolized by(F^), as for dolls the maximum values are denoted by the symbol (F *)

1.The support of the decision-maker for requirement Building cyber resilience:assuming that the decision-maker supports Building cyber resilienceand that the relative importance is 50% , while the rest of the requirementstake 50% according to the priorities Table (7) showsas follows :

Iteam	requirement	Possibility %	Development		construction	
			F*	F^	F*	F^
1.	Building cyber resilience	50	1	1	0	0
2.	Enhancing global cooperation	4.9*	0	0	1	1
3.	Understanding Future	7.3	0	0	1	1

	Networks and Technology					
4.	Cybersecurity awareness	1.9	1	1	<u>0</u>	0
5.	Cybersecurity governance and risk management	7.8	0	0	1	1
6.	Developing new rules and legislation	3	0	1	0	1
7.	International Cooperation	14.6	0	0	1	1
8.	Integration of more than one characteristic	4.3	0	0	1	1
9.	Back to traditional technology	4.9	0	0	1	1 *best lowest
10	Cyber risk insurance	1.3	0	0	1	1
Total			0.519	0.549	0.450	0.480

*Probability = relative importance of the requirement / total weights - the relative importance of the excluded requirement * 50

The largest benefit (F*)9is 0.51 (development))

The lowest value of benefit(F^) is 0 .480 (construction)   **D > C**   So the development offer is the best

2.**Supporting the decision**-maker for requiremen gl**obal cooperation:** assuming that the decision-maker supports for requiremen and that the relative importance of the is 50% , while the rest take %50 for requirementsaccording to the priorities Table(8) showsas follows :

Iteam	requirements	Possibility %	Development		Construction	
			F*	F^	F*	F^
1.	Building cyber resilience	0.012	1	1	0	0
2.	Enhancing global	0.50	0	0	1	1

	cooperation					
3.	Understanding Future Networks and Technology	0.078	0	0	1	1
4.	Cybersecurity awareness	0.022	1	1	0	0
5.	Cybersecurity governance and risk management	0.084	0	0	1	1
6.	Developing new rules and legislation	0.03	0	1	0	1
7.	International Cooperation	0.157	0	0	1	1
8.	Integration of more than one characteristic	0.047	0	0	1	1
9.	Back to traditional technology	0.052	0	0	1	1 *best lowest
10	Cyber risk insurance	0.013	0	0	1	1
Total			0.034	0.064	0.931	0.961

The largest value o

benefit (F*).is 0 931(construction

The lowest value of benefit (F^) is 0.064   (development)   C > **D**
So the construction offer is the best

3.Decision-making support for understanding future technology networks: Assuming that the decision-maker supports the understanding of future technology networks by 50%, and by calculating the relative importance of the rest of the characteristicsTable (9) shows as follows:

Iteam	requirements	Possibility %	Development		New system	
			F*	F^	F*	F^
1.	Building cyber resilience	0.012	1	1	0	0

2.	Enhancing global cooperation	0.048	0	0	1	1
3.	Understanding Future Networks and Technology	0.50	0	0	1	1
4.	Cybersecurity awareness	0.022	1	1	0	0
5.	Cybersecurity governance and risk management	0.084	0	0	1	1
6.	.Developing new rules and legislation	0.03	0	1	0	1
7.	International Cooperation	0.157	0	0	1	1
8.	Integration of more than one characteristic	0.047	0	0	1	1
9.	Back to traditional technology	0.052	0	0	1	1 *best lowest
10	Cyber risk insurance	0.015	0	0	1	1
Total			0.034	0.064	0.903	0.933

The largest value of benefit (F*).is 0 903(construction)   lowest value of benefit(F^) is 0.064   development))   **C > D**   So the construction offer is the best

4.Decision-making support for Cybersecurity awareness : Assuming that the decision-maker supports for Cybersecurity awareness by 50%, and by calculating the relative importance of the rest of the characteristicsTable (10) shows as follows:

Iteam	requirements	Possibility %	Development		New system	
			F*	F^	F*	F^

1.	Building cyber resilience	0.012	1	1	0	0
2.	Enhancing global cooperation	0.05	0	0	1	1
3.	Understanding Future Networks and Technology	0.074	0	0	1	1
4.	Cybersecurity awareness	0.50	1	1	0	0
5.	Cybersecurity governance and risk management	0.079	0	0	1	1
6.	Developing new rules and legislation	0.03	0	1	0	1
7.	International Cooperation	0.148	0	0	1	1
8.	Integration of more than one characteristic	0.044	0	0	1	1
9.	Back to traditional technology	0.05	0	0	1	1 *best lowest
10	Cyber risk insurance	0.014	0	0	1	1
Total			0.512	0.542	0.459	0.489

The largest benefit (F*)2is 0.51 (development))

The lowest value of benefit(F^)is 0.489 (constructio)   **D > C**
So the development offer is the best

5.Decision-making support for Cybersecurity governance and risk management : Assuming that the decision-maker supports for Cybersecurity governance and risk management by 50%, and by calculating the relative importance of the rest of the characteristics Table (11) shows as follows:

Iteam	requirements	Possibility %	Development		New system	
			F*	F^	F*	F^
1.	Building cyber resilience	0.012	1	1	0	0
2.	Enhancing global cooperation	0.05	0	0	1	1
3.	Understanding Future Networks and Technology	0.074	0	0	1	1
4.	Cybersecurity awareness	0.025	1	1	0	0
5.	Cybersecurity governance andrisk management	0.50	0	0	1	1
6.	.Developing new rules and legislation	0.034	0	1	0	1
7.	International Cooperation	0.168	0	0	1	1
8.	Integration of more than one characteristic	0.05	0	0	1	1
9.	Back to traditional technology	0.056	0	0	1	1 *best lowest
10	Cyber risk insurance	0.015	0	0	1	1
Total			0.037	0.071	0.913	0.947

The largest value of benefit (F*)is 0.913 construction)

The lowest value of benefit(F^)is 0.071   development)   C > D
So the construction offer is the best

6.Decision-making support for Developing new rules and legislation   : Assuming that the decision-maker supports for Developing new rules and legislation by 50%, and by calculating the relative importance of the rest of the characteristicsTable (12) shows as follows:

Iteam	requirements	Possibility %	Development		New system	
			F*	F^	F*	F^
1.	Building cyber resilience	0.012	1	1	0	0
2.	Enhancing global cooperation	0.05	0	0	1	1
3.	Understanding Future Networks and Technology	0.075	0	0	1	1
4.	Cybersecurity awareness	0.021	1	1	0	0
5.	Cybersecurity governance and risk management	0.081	0	0	1	1
6.	.Developing new rules and legislation	0.5	0	1	0	1
7.	International Cooperation	0.151	0	0	1	1
8.	Integration of more than one characteristic	0.05	0	0	1	1
9.	Back to traditional technology	0.051	0	0	1	1 *best lowest
10	Cyber risk insurance	0.033	0	0	1	1
Total			0.033	0.533	0.491	0.991

The largest valu benefit (F*).is 0 .491) construction)

 The lowest value of benefit(F^)is 0.533   development)   C > **D**
So the construction offer is the best

7.Decision-making support for International Cooperation : Assuming that the decision-maker supports for International Cooperation by 50%, and by calculating the relative importance of the rest of the characteristics Table (13) shows as follows:

Iteam	requirements	Possibility %	Development		New system	
			F*	F^	F*	F^
1.	Building cyber resilience	0.016	1	1	0	0
2.	Enhancing global cooperation	0.066	0	0	1	1
3.	Understanding Future Networks and Technology	0.099	0	0	1	1
4.	Cybersecurity awareness	0.027	1	1	0	0
5.	Cybersecurity governance and risk management	0.107	0	0	1	1
6.	.Developing new rules and legislation	0.04	0	1	0	1
7.	International Cooperation	0.50	0	0	1	1
8.	Integration of more than one characteristic	0.061	0	0	1	1
9.	Back to traditional technology	0.066	0	0	1	1 *best lowest
10	Cyber risk insurance	0.019	0	0	1	1
Total			0.043	0.083	0.884	0.958

The largest value o benefit (F*.is 0.884 construction)

The lowest value of benefit(F^)is 0.83   development)   C > **D**
 So the construction offer is the best

 8.Decision-making support fo Integration of more than one characteristic : Assuming that the decision-maker supports for Integration of more than one characteristic by 50%, and by calculating the relative importance of the rest of the characteristicsTable (14) shows follows:

Iteam	requirements	Possibility %	Development		New system	
			F*	F^	F*	F^
1.	Building cyber resilience	0.012	1	1	0	0
2.	Enhancing global cooperation	0.05	0	0	1	1
3.	Understanding Future Networks and Technology	0.078	0	0	1	1
4.	Cybersecurity awareness	0.022	1	1	0	0
5.	Cybersecurity governance and risk management	0.084	0	0	1	1
6.	.Developing new rules and legislation	0.032	0	1	0	1
7.	International Cooperation	0.156	0	0	1	1
8.	Integration of more than one characteristic	0.50	0	0	1	1
9.	Back to traditional technology	0.051	0	0	1	1 *best lowest
10	Cyber risk insurance	0.014	0	0	1	1
Total			0.043	0.066	0.933	0.965

The largest value o benefit (F*.is 0.933 construction)

The lowest value of benefit(F^)is 0.066   development))   C > **D**
So the construction offer is the best

 9.Decision-making support for Back to traditional technology: Assuming that the decisi on-maker supports for   Back to traditional technology   by 50%, and by calculating the relative importance of the rest of the characteristicsTable (15) show as follows:

Iteam	requirements	Possibility %	Development		New system	
			F*	F^	F*	F^
1.	Building cyber resilience	0.012	1	1	0	0
2.	Enhancing global cooperation	0.05	0	0	1	1
3.	Understanding Future Networks and Technology	0.078	0	0	1	1
4.	Cybersecurity awareness	0.022	1	1	0	0
5.	Cybersecurity governance and risk management	0.084	0	0	1	1
6.	.Developing new rules and legislation	0.032	0	1	0	1
7.	International Cooperation	0.157	0	0	1	1
8.	Integration of more than one characteristic	0.047	0	0	1	1
9.	Back to traditional technology	0.50	0	0	1	1 *best lowest
10	Cyber risk insurance	0.015	0	0	1	1
Total			0.034	0.066	0.933	0.965

 The largest value of benefit F*.is 0.933(cconstruction)

The lowest value of benefit(F^)is 0.066 development))   C > **D**
So the construction offer is the best

10.Decision-making support for Cyber   risk insurance   : Assuming that the decision-makersupports the Cyber risk insurance by 50%, and by calculating the relative importance of the rest of the characteristics Table (16) shows as follows:

Iteam	requirements	Possibility %	Development		New system	
			F*	F^	F*	F^
1.	Building cyber resilience	0.011	1	1	0	0
2.	Enhancing global cooperation	0.05	0	0	1	1
3.	Understanding Future Networks and Technology	0.073	0	0	1	1
4.	Cybersecurity awareness	0.02	1	1	0	0
5.	Cybersecurity governance and risk management	0.078	0	0	1	1
6.	Developing new rules and legislation	0.029	0	1	0	1
7.	International Cooperation	0.146	0	0	1	1
8.	Integration of more than one characteristic	0.044	0	0	1	1
9.	Back to traditional technology	0.049	0	0	1	1 *best lowest
10	Cyber risk insurance	0.50	0	0	1	1
Total			0.031	0.06	0.940	0.969

The largest value benefit (F*.is 0.940 construction)

 The lowest value of benefit(F^)is 0.06 development))   C > D
So the construction offer is the best

4/3The decision to choose the best alternative through previous impact supportmodels
A group of alternatives has been presented to the decision-maker, so he only has to nominate the alternative that suits his preference, and he will choose one of the following modelsTable (17) shows :

Iteam	requirements	largest value	Development		Construction	
			F*	F^	F*	F^
1.	Building cyber resilience	D	0.519	0.549	0.450	0.480
2.	Enhancing global cooperatio	C	0.034	0.064	0.931	0.961
3.	Understanding Future Networks and Technology	C	0,034	0.064	0.903	0.933
4.	Cybersecurity awareness	D	0.512	0.592	0.459	0.489
5.	Cybersecurity governance andrisk managemen	C	0.037	0.071	0.913	0.947
6.	Developing new rules and legislation	C	0.033	0.533	0.491	0.991
7.	International Cooperation	C	0.043	0.083	0.884	0.958
8.	Integration of more than one characteristic	C	0.043	0.066	0.933	0.965
9.	Back to traditional technology	C	0.043	0.066	0.933	0.965
10.	Cyber risk insurance `	C	0.031	0.06	0.940	0.969

It is clear from the above table that the multi-characteristic utility theory offers a set of possibilities that. helps the decision-maker in making his decision to support a specific requirement or even without any personal wisdom to make the appropriate decision, and generally, the decision-maker can also support more than one requirement and that depends on his experience, The above table shows that cybersecurity requirements (1 and 4) can develop the existing information system by introducing new mechanisms for the system, and this is evidence that the decision analysis models are correct, as they do not deserve to replace the entire system, and as for the other requirements, they require changing the system: **Therefore , the second hypothesis was accepted that the best alternative was construction information system to confront the cyber threat .**

The fourth topic

CONCLUSIONS AND RECOMMENDATIONS

First conclusions: Iraqi banks face cyber threats that may stand unable to find solutions to stop them, recover from them, and return to a state before the failure occurred, and accordingly the research focused on cyber security requirements approved by the World Economic Forum, and the researcher added to them suggested requirements(Integration of more than one characteristic, Back to traditional technology , Cyber risk insurance) , All this in order to make the decision-maker in the Trade Bank of Iraq fully select, in choosing and supporting his decision to suit what he faces to match ,to choose the best alternatives based on his experience and personal judgment and support for any of the requirements.

1.Rejection of the current information system for its inability to bridge the gaps facing the cyber threat.

 2.The relative importance of cyber security requirements for choosing amanagement   information system is not equal according to the desires and experiences of the decision-maker, so what he considers the requirement (1) is the most important may be given by a beneficiary another one is less important, depending on the circumstances surrounding the decision-maker.

3. The use of quantitative methods provides a set of models that help the decision-maker to make his decision in all possibilities.

4. The study proved that there are requirements that do not necessitate replacing the entire system, paragraphs (1,4))as they can be developed through the introduction of mechanisms commensurate with those requirements. As for the other requirements, they are basic and require the construction of a new system for the table (17), and this shows that the decision analysis models are correct .

RECOMMENDATIONS: THE RECOMMENDATIONS OF THE RESEARCH ARE AS FOLLOWS:

1. The strategy of cybersecurity in Iraq has not been implemented, which exposes various sectors to danger, including the Iraqi Trade Bank, to cyberattacks. Therefore, mechanisms must be put in place to implement them and a central authority should be established to supervise all sectors and complementary work, not scattered.

2.The Trade Bank of Iraq shall take into account the costs and benefits when developing or establishing a management information system.

3.The indicator for measuring the implementation of the cyber risk standards of the World Economic Forum showed a significant decline, as Iraq recorded the rank (129) globally and (17) in the Arab world, and this requires those in charge of cyber security to implement the procedures.

4.Building a digital risk management to which all units (information security, networks, infrastructure, applications, ...) are linked at the level of other departments and linked to senior management, integrated to confront the cyber threat.

REFERENCE

[1] Economic Forum, Centre. 1 Cybersecur http://bit.ly/3ZEz8ZC
[2] Defense Cyber Security Market: Growth, Trends, Covid-19 Impact, and Forecasts (2023 –2028)https://bit.ly/3imO51z

[3] $44.7 billion cybersecurity market in the   region by 2027, day7, August 17, 2022, https://bit.ly/3iqC8a

[4] Diab, Mohamed Abdel-Wahhab Ibrahim, 2017, "Studying the relationship between administrative re-engineering and decision-making support systems: application to Egyptian banks," Scientific Journal of Economics and Commerce, Faculty of Commerce, Ain Shams University, October, pp.65-86.

[5] World Economic Forum, Centre for Cybersecur   http://bit.ly/3ZEz8ZC

[6] Erskine, Michael A. ; Gregg, Dawn G. ; Karimi, Jahangir & Judy E. Scott, (2019) , "Individual Decision Performance Using Spatial Decision Support Systems ",InformationSystemsFrontiers,Springer,Vol.21,pp.1369–1384

[7] Turban,E; Sharda,R; Delen,D; Aronson,J; Liang , T; King, D,(2011) " Decision support and business intelligence systems" ,Pearson Education ,In New Jersey ,USA

[8] Erskine, Michael A. ; Gregg, Dawn G. ; Karimi, Jahangir & Judy E. Scott, (2019) , "Individual DecisionPerformance Using Spatial Decision Support Systems   :A Geospatial Reasoning Ability and Perceived Task Technology Fit Perspective" ,Information Systems Frontiers,Springer,Vol.21,pp.1369–1384.

[9] Bani Mustafa, Suhail Mohamed Hassan (2013), "The Impact of Using Decision Support Systems on Performance Development in Jordanian Commercial Banks," The Arab Journal of Administrative and Economic Studies, The Arab Center for Studies and Research, January,Volume/Issue:1,pp.29-46

[10]Galipalli, Ashwin Kumar & Madyala, Haritha Jyothi, (2012), " Process to Build an Efficient Decision Support System: Identifing Important Aspects of A DSS" ,Master's (one year) thesis in Informatics, University of BORAS,Spring.

[11]Al-Lawzi, Amani Samir (2015), "The Impact of Using Decision Support Systems on Achieving Competitive Advantage: An Empirical Study on Jordanian Commercial Banks," Master Thesis, Faculty of Business, Amman Arab University, Jordan.

[12]Galipalli, Ashwin Kumar & Madyala, Haritha Jyothi, (2012), " Process to Build an Efficient Decision Support System: Identifing Important Aspects of A DSS" ,   Master's   (one year)thesis in Informatics, University ofBORAS,Spring

[13]Wilson. Charles E. (2014): Cyber security education the emergence of an accredited academic discipline. Journal of the colloquium information system Security education. 2 (1).213

[14]Mustafa ,Islam Juma Mustafa, 2021 ,The crime of breaching cybersecurity and protecting the use of data and information in Egyptian law The Legal Journal (a journal specialized in legal studies and research) : 2537 - 0758 , p.724.

[15]Council of Ministers - National Security , Iraqi Cyber Security Strategy 22-2025.pp.13

[16]ITU (2022): Global cybersecurity Index (GCI) 2021 – Studies & researc United Nations Economic and Council.United Kingdom. :

[17]Mahmoud Shamkhi , the Cybersecurity Index and Iraq's Position in it,21.6.2022 ,College of Administration and Economics - Karbala University - Artical 23.Jan.2023

[18]World Economic Forum, Centre for Cybersecur   http://bit.ly/3ZEz8ZC

[19]myriam-Dunn Caveltry, "Cyber-Security," In Alan Collins (ed.), Contemporary Security Studies, 5th edition (Oxford: New York: Oxford University Press, 2019), pp. 374-375.

[20]Mohammed Al Kuwaiti, Divergent Trends in Cybersecurity: The CyberPulse Initiative.. Case Study, Lecture Papers (3), Abu Dhabi: Trends Center for Research and Consultation, September 2022

[21]Klaus Schwab,The Fourth Industrial Revolution, (New York, NY: Crown Busines,2017

[22]myriam-Dunn Caveltry, "Cyber-Security," In Alan Collins (ed.), Ibid,   2019, p. 375

[23]Aloysius Chiang, "The UAE Focuses on Cybersecurity to Meet the Requirements of the Digital Age," Al Bayan Newspaper, October 19, 2022. https://bit.ly/3Qjn9M.

[24]Raj M. Shah, Chairman of Resilience Insurance and Managing Partner at Shield Capital.https://www.independentarabia.com/anuary/9/February2022.

[25]Kiran Sridhar is a researcher at the Center for Risk Studies at the University of Cambridge. Foreign Affairs,https://www.independentarabia.com/ January/February 2022