The Impact of Knowledge Management on Reducing Digital Crime Levels: Analytical study in the Iraqi Ministry of Interior

[1*]Lamia Salman Al-Zubaidi, [2]Arwa Ahmed Abdel Wahab

[1]Professor, College of Administration and Economics, Al-Mustansiriya University, Baghdad, Iraq.
Lamyaasalman@yahoo.com
[2]Researcher College of Administration and Economics, Al-Mustansiriya University, Baghdad, Iraq.
ahmedarwa331@gmail.com

Abstract

This study aims to identify knowledge management and digital crimes for government security organizations, and to know the roles that are embodied in raising the performance of organizations, although there is no agreement on the concept of knowledge management and digital crimes, but there are agreements by some writers and researchers about its application because it enhances the efficiency of the performance of any organization Whether it is private, different or governmental, as any organization implements it supports its ability to face any crises that occur from the external environment, and the importance of knowledge management has emerged as an effective tool for continuous improvement in all organizations through a set of external and internal mechanisms, and among the most important electronic crimes that aim To address knowledge management are (crimes of women and children trade, crimes of electronic digital commerce, administrative corruption in all its forms, assault on the privacy of individuals, theft of information and services, information piracy, electronic terrorism, sabotage, abuse and theft of computers (viruses, ... etc.).

Keywords: Digital crimes, government security, knowledge management, women and children trade, corruption.

INTRODUCTION

Organizations began seeking to develop their products or services that they provide to customers. They also began to compete with other organizations with productivity or common services, and try to own modern technologies with special specifications that lead to the improvement and development of their operations to be more efficient and effective, as well as seeking also to increase the preparation of Human cadres who have the ability to deal and act with these new technologies, find appropriate solutions to all the problems facing the organization, develop them intellectually and practically, and raise awareness of these cadres and the community about the importance of advanced technology represented in knowledge management.

Firstly: The problem of the study

The problem of the study is based on the premise of: "there is a decrease in the level of application of the principles of knowledge management, which necessitates the need to focus on developing digital skills to deal with the risks and challenges of electronic transactions."

Second: The importance of the study

The importance of the study follows from the importance of the variables in question, as it is an attempt to arouse interest in the researched organization through its leaders and affiliates, and the prominent roles they play and the results of adopting the application of knowledge management and the ability of its impact to achieve digital crimes and its profound effects on society.

Third: Objectives of the study

The study seeks to push the research organization to apply knowledge management in order to identify the level and type of relationship between knowledge management and digital crimes.

Fourth: The hypotheses of the study

First: The main hypothesis of the study: The adoption of a knowledge management system leads to addressing the challenges and reducing the risks of digital crimes occurring in the Ministry of Interior.

Second, the correlation hypotheses

The main hypothesis of the H1 correlation:

There is a significant correlation between knowledge management and digital crimes, and the following sub-hypotheses are branched from it:

H(1-1) :- There is a significant correlation relationship between knowledge management and digital crimes, and the following secondary hypotheses are branched from it: -

H(1-1-1) :- There is a significant correlation between knowledge management and information

H(1-1-2) :- There is a significant correlation between knowledge management and electronic devices

H(1-1-3) :- There is a significant correlation between knowledge management and people or entities

Third: Impact hypotheses

The main hypothesis of the effect H2: There is a significant effect of knowledge management in digital crimes, from which the following sub-hypotheses are branched:

H(2-1) :- There is a significant effect of knowledge management in digital crimes, and the following secondary hypotheses are derived from it:

H(2-1-1) :- There is a significant effect of knowledge management in information

H(2-1-2) :- There is a significant effect of knowledge management in electronic devices

H(2-1-3) :- There is a significant effect of knowledge management on people or entities

Fifth: Study Methodology

This study relied on the descriptive and analytical approach as it is one of the most prominent approaches that are used in practical studies in order to identify the phenomenon of the study. The study was divided according to the following:-

First: The theoretical framework of the study (defining the study variables)

1-Knowledge management: Knowledge management is a set of legal principles and rules whose purpose is to protect people as defined in international and national law. In the case of being attacked by others, whether from within or from abroad (United Nations, 2018), international legitimacy has brought benefit to the protection of human rights in general and, as a consequence, it has become a source for the rulings of many national laws. The Iraqi project has dealt with the right of individuals to their personal freedom And a safe protection for his life through external and internal dangers, he began by specifying penalties for perpetrators and limiting them by imposing on them the penalty of criminalization (deterrence) (Salah al-Din, 2008: 95). Digital crimes are among the most serious crimes that threaten society, and it is difficult to protect them, And the fact that it depends on accuracy, speed and concealment in the event of its commission, as well as its multiplicity and diversity in abundance and not being familiar with it or confining it to a specific place and characterized by speed and continuous development (Khalifa, Hammoud, 2019 : 148), these crimes occur through the Internet, as they defraud people through means such as advertising pictures or advertisements for some products, clothes, or good treatments and others, from misleading propaganda on their part, and this is what helps them to reach and seize secret numbers or know Their secret numbers for their amounts (Ali, 2003: 493), most international legislation seeks to punish the perpetrators who violate the secrets of the organizations or commit the crimes of infringing on the organization’s websites or hacking and stealing data and information (Hijazi, 2008: 52), the Iraqi project defined these crimes Whoever deliberately enters without permission or permission a website or an information system or has been in contact with computer systems or parts thereof (Article 14, 2010). For the security of the organization (Article 1: 2004), penal protections must be provided for the private lives of individuals who infringe on the means of information technology, as it has become one of the most important requirements of government organizations and the most important A mechanism to achieve electronic security from extremists who steal information and data, and therefore it must have deterrent laws that guarantee its protection and combat modern electronic crimes and achieve the protection of people’s interests from all electronic digital crimes. (Hadii Ahmed, 2018: 160).

2-Information:: It is the facts, messages, instructions, and concepts that are presented in a real way that is valid for the purpose of reporting, communicating and interpreting by an individual or individuals to other individuals (Al-Arian, 2004: 36). Or deducing what can be inferred from it alone or intertwined with others or interpreting it as it gives an explanation and knowledge to decision-makers and how to help them in making a sound judgment on phenomena or actively contributing to the development of theoretical or applied knowledge (Shta, 2001: 62), and in this case it included digital crimes Electronic cases of theft or change of original information or permanent deletion of information, for example in the case of criminal activity whose main objective is to hack e-mail or access the computer and tamper with all its contents, or steal necessary data and information of importance stored on the site and benefit from it, including violations The organization's privacy, its intellectual property rights and the information it possesses of competitive value and other modes of action Another water. (Al-Malt, 2006: 167)

3-Electronic devices: This is the most prevalent case, as the National Center for the American Computer has mentioned that there are programs that attack and infect a group of computer systems with large types and methods of vital viruses that infect humans, as these programs roam the computer looking for uninfected passive programs. The presence of copies on their own to enter it, after which the infected programs start executing the virus’s commands, and it has superior characteristics and capabilities for rapid disappearance, spread, difference and the ability to destroy and destroy entire computer systems (Salama, 2008: 155), and digital crimes in this case included disabling Computers or permanently destroying them by sending viruses or programs that contain offensive systems that damage computer systems, which leads to the paralysis of all activities related to the device or its associated systems, (Tammam, 2009: 270).

4-Persons or entities: It is the right of persons, organizations, or groups to determine for themselves how, when and to what extent information can reach other parties, how they are reached, and any type orally, in writing or in a form (Bogdain, 2019: 65), and this case represents the personal domain The e-mail is for every party affiliated to a person or organization and is limited to them and others have no right to interfere in it (Khalifeh, 2019: 41), as well as diagnosing large categories of digital and electronic crimes for individuals, organizations or entities directly or indirectly, such as threats, extortion or thefts, and an example of This is through the Internet, money is stolen using bank card numbers belonging to others, or instructions that carry terrorist instructions directed against their members, organizations or certain parties who are threatened through the Internet from the same country or from abroad (Al-Janayi, Al-Janayi, 2005: 77).

Second: The practical framework (tests of validity and reliability of the questionnaire with its variables and sub-dimensions)

Honesty and reliability are among the conditions that must be provided in the questionnaire to become eligible to be used in the analytical study. Two tests are used in the study to prove the validity of the paragraphs of the questionnaire, represented by the apparent honesty, and the reliability coefficient (Cronbach's Alpha) to prove the reliability of the data obtained from the questionnaire.

1-First: Validity tests for resolution

The questionnaire’s apparent validity test: It means the ability of the questionnaire to measure the research variables that the questionnaire was designed to measure.

Table 1.0 *The results of the apparent validity test of the questionnaire*

Study variables	**The number of items in the questionnaire**	**The number of paragraphs agreed upon by the arbitrators**	**The percentage of the professors’ agreement**	**Validity level**	**Researcher's comment**
X3 knowledge management	7	7	100%With some grammatical correction	Higher	The presence of high apparent validity in the knowledge management paragraphs within electronic governance
X electronic governance	7	7		Higher	The presence of high apparent validity in the electronic governance paragraphs
Y1 Informations	8	8	100%With some grammatical correction	Higher	The presence of high apparent validity in the information paragraphs within the reduction of electronic crime levels
Y2 electronic devices	8	8	100%With some grammatical correction	Higher	The presence of high apparent validity in the paragraphs of electronic devices within the reduction of levels of electronic crime
Y3 persons or entities	7	7	100%With some grammatical correction	Higher	The presence of high apparent validity in the paragraphs of persons or entities within the reduction of cybercrime levels
Y Reducing levels of digital crime	23	23	100%With some grammatical correction	Higher	The presence of high apparent validity in the paragraphs of the levels of electronic crime
All paragraphs of the questionnaire	44	44	100%	Higher	The presence of high apparent validity in all paragraphs of the questionnaire

Table (1) shows in detail that the apparent sincerity was achieved in the paragraphs of the questionnaire, as it is noted from the table that the percentage of the arbitrators’ agreement on the sincerity of the paragraph of the knowledge management variable amounted to (100%), which is a large percentage that documents the agreement of the arbitrators on (7) paragraphs among 7) A paragraph representing knowledge management (the independent variable) with its dimension represented by knowledge management, while the percentage of the arbitrators' agreement on the sincerity of the paragraphs of the dimensions of the variable reducing levels of electronic crime (the responsive variable) reached (100%), which is a large percentage that shows the agreement of the arbitrators on (23) a paragraph out of (23) paragraphs that represented the variable of reducing cybercrime levels in its three dimensions (information.electronic devices,people orentities), while the percentage of the arbitrators' agreement on the sincerity of all the paragraphs of the questionnaire was recorded (100%), which is a large percentage confirming the agreement of the arbitrators on (44) paragraphs out of(44) paragraphs.

2- Resolution stability test: by reliability, it means that if the scale is applied to the same group of individuals after a period of time, it will give the same results. (70%), and this means that the research questionnaire with its different scales is highly stable and can be adopted at different times for the same individuals and gives the same results.

Table 2.0 *Shows the stability of the questionnaire variables in their detailed form.*

Researcher's comment	stability level	Cronbach's Alpha . Resolution Stability Coefficient Value	The number of items in the questionnaire		
The presence of high stability in knowledge management within electronic governance	Higher	**0.878**	**7**	knowledge management	X2
The presence of high stability in the paragraphs of the task priority matrix	Higher	0.874	7	electronic governance	X
There is good stability in the information paragraphs within the defined time variable	Good	0.730	8	Informations	Y1
There is good stability in the paragraphs of electronic devices within the variable of reducing levels of electronic crime	Good	0.786	8	electronic devices	Y2
The presence of high stability in the paragraphs of people or entities within the variable of reducing cybercrime levels	Higher	0.809	7	persons or entities	Y3
The presence of high stability in the paragraphs of reducing cybercrime levels	Higher	0.834	23	Reducing levels of digital crime	Y
The presence of high stability in all paragraphs of the questionnaire	Higher	0.957	44	All paragraphs of the questionnaire	

Source: Prepared by the researcher based on the results of the statistical analysis of the questionnaire using the statistical program spss v.28.

It is evident from Table (2) that the values of Cronbach's Alpha stability coefficient for the dimensions of the independent variable knowledge management amounted to (0.878), which is higher than the minimum permissible, and this means that this dimension is stable and can be adopted at different times for the individuals themselves and give the same results, and this means The independent variable with its seven measures has high stability and can be adopted at different times for the same individuals and gives the same results, while the values of Cronbach's Alpha stability coefficient for the dimensions of the responsive variable reduce the levels of electronic crime (information, electronic devices, people or entities) respectively (0.730, 0.786, 0.809), which is higher than the minimum permissible, which means that these dimensions are highly stable and can be adopted at different times for the same individuals and give the same results, while the values of Cronbach's Alpha stability coefficient for the responsive variable (reducing levels of cybercrime) in total (0.834), which is higher than the minimum, which means that the responsive variable with its twenty-three measures is highly stable and can be adopted at different times for the same individuals and gives the same results.

3-Description of the research sample and presentation and analysis of the results of the field research

This topic deals with two axes. The first axis includes a description of the research sample (officials in the Ministry of Interior) in terms of their demographic variables, as well as some functional variables. While the second axis includes a description and diagnosis of the research variables, analysis of the sample answers, and interpretation of the results.

Third: Testing the research hypotheses

Testing the correlations between the research variables

Analysis of the hypothetical research scheme requires testing its main and sub-hypotheses according to their occurrence in the research methodology. Using the simple correlation coefficient (Spearman), which is one of the statistical methods used to measure the strength and direction of the relationship between two variables using the ready-made statistical program (SPSS) version 28.

In order to analyze the nature of the relationships between those variables, the Spearman rank correlation coefficients were calculated to check the existence of the relationship, as shown in the following table (3):

Table 3.0.. *Spearman rank correlation coefficients to examine the existence of the relationship between knowledge management (knowledge management) and the reduction of cybercrime levels.*

The strength and direction of the relationship	**Sig. (2-tailed)**	**Spearman's Simple Correlation Coefficient**	**Variables**		**Hypothesis**
			transponder	**independent**	
strong direct	(0.00)	0. 751**	Reducing levels of digital crime	3-1 knowledge management	Sub
centrifugal medium	(0.00)	0.694**	Reducing levels of digital crime	e-governance	first principal

Source: The results of the statistical analysis using the statistical program spss v.28.

Table (3) indicates that there is a medium significant correlation relationship at the level of significance Sig. (2-tailed) (0.00), i.e., with a confidence level of 100% between knowledge management and the reduction of cybercrime levels, where the value of the Spearman rank correlation coefficient reached 0.694)) and this result indicates the existence of a moderately strong direct correlation between knowledge management and the reduction of levels of cybercrime.

Note: The symbol * means that the value of the correlation coefficient is significant at the level of significance (0.05), and the symbol ** means that the value of the correlation coefficient is significant at the level of significance (0.01).

The following is the analysis of the sub-relationships between the matrix after knowledge management (knowledge management) and the reduction of digital crime levels at the level of sub-hypotheses.

1-1 Analyzing the relationship between knowledge management and reducing cybercrime levels.

In Table (3), we note that the value of the correlation coefficient between knowledge management and the reduction of cybercrime levels has reached (0.751), which is a strong significant and direct correlation at the level of significance (0.00)) Sig. (2-tailed), i.e. with a confidence limit of 100%, and this result indicates that the greater the interest in knowledge management, the more this leads to an increase in the level of reducing cybercrime levels, meaning that reducing cybercrime levels can be generally enhanced by just making a positive change in the management of cybercrime. Knowledge, and this result supports the third sub-hypothesis of research emanating from the first main hypothesis, and this means acceptance of this hypothesis, that is, there is a significant correlation with statistical significance, knowledge management and the reduction of cybercrime levels.

The following is an analysis of the secondary relationships between the knowledge management dimension and the dimensions of reducing digital crime levels and at the level of secondary hypotheses, as shown in the following table (49).

Table 4.0 ..*Spearman rank correlation coefficients to examine the existence of the relationship between knowledge management and the dimensions of reducing cybercrime levels.*

The strength and direction of the relationship	**Indication level Sig.(2-tailed)**	**Spearman's Simple Correlation Coefficient**	**Variables**		**Hypothesis**	
			transponder	**independent**		
strong direct	(0.00)	0 .781 **	the information	knowledge management	1-3-1	high school
centrifugal medium	(0.00)	0.593**	electronic devices		2-3-1	
strong direct	(0.00)	0 .720 **	persons or entities		3-3-1	

Source: The results of the statistical analysis using the statistical program spss v.28.

1-1-1.Analyze the relationship between knowledge management and information.

In Table (4), we note that the value of the correlation coefficient between knowledge and information management has reached (0.781), which is a strong significant and direct correlation at the level of significance (0.00) Sig. (2-tailed), that is, with a confidence limit of 100%, and this result indicates that the greater the interest in knowledge management, the more this leads to an increase in the level of information dimension within the reduction of levels of cybercrime, and this result supports the first secondary research hypothesis emanating from the third sub-hypothesis. This means accepting this hypothesis, that is, there is a significant statistically significant correlation between knowledge and information management.

1-1-2.Analysis of the relationship between knowledge management and electronic devices.

In Table (4), we note that the value of the correlation coefficient between knowledge and information management amounted to (0.593), which is a significant and direct medium correlation at the level of significance (0.00) Sig. (2-tailed), i.e., with a confidence limit of 100%, and this result indicates that the greater the interest in knowledge management, the more this leads to an increase in the level of interest in electronic devices within the reduction of cybercrime levels, and this result supports the second secondary research hypothesis emanating from the third sub-hypothesis This means that this hypothesis is accepted, that is, there is a significant statistically significant correlation between knowledge management and electronic devices.

1-1-3. Analysis of the relationship between knowledge management and people or entities.

In Table (4), we note that the value of the correlation coefficient between knowledge management and people or entities has reached (0.720), which is a strong significant and direct correlation at the level of significance (0.00) Sig. (2-tailed), that is, with a confidence limit of 100%, and this result indicates that the greater the interest in knowledge management, the more this leads to an increase in the level of interest in people or entities within the reduction of cybercrime levels, and this result supports the third secondary research hypothesis emanating from the sub-hypothesis Third, and this means accepting this hypothesis, that is, there is a significant statistically significant correlation between knowledge management and people or entities.

2- Testing the effect between the research variables

This paragraph seeks to test the second main research hypothesis related to testing the effect between the research variables: knowledge management (the independent variable), reducing levels of cybercrime (the responsive variable) and the hypotheses subordinate to it using Simple Linear Regression analysis.

Table 5.0 *Table of variance analysis of the knowledge management regression equation in reducing digital crime levels n=265.*

The coefficient of determination R2 % Interpretation ratio	Fixed limit α	beta regression coefficient	Indication level Sig. (2-tailed)	F- test	Variables		Hypothesis
					Transponder	Independent	
54.4%	1.749	0.764	(0.00)	313.712	Reducing levels of digital crime	knowledge management	3-2 Sub-
41.3%	1.571	0.491	(0.00)	185.031	Reducing levels of digital crime	electronic governance	first principal

Source: The results of the statistical analysis using the statistical program spss v.28.

Table (5) shows the values of the F-test for the model as a whole. The value of the F-test in relation to the effect of knowledge management in reducing levels of cybercrime was (185.031), with a significance level of Sig*. (2-tailed) (0.00), and this means that there is a significant effect of knowledge management in reducing cybercrime levels at a confidence level of (100%), and the value of the constant is (1.571 (=), which means that there is a presence of (knowledge management) what Its amount is (1.571) in the directors of the Ministry of Interior, even if the reduction of cybercrime levels is zero, and the value of a coefficient (which represents the value of the slope of the regression line (0.491), which is interpreted as the amount of change in the value of the respondent variable when a change of one unit in the value of The independent variable, that is, increasing the value of the knowledge management variable by one unit will lead to a change of (0.491) in reducing cybercrime levels, and the value of the coefficient of determination (R2) of (0.413), which means that (41.3%) of the variance occurred in reducing The levels of cybercrime is a variation explained by the knowledge management that entered the model, and that (59.7%) is a variation explained by factors that did not enter the regression model of the current study, so accept the second main hypothesis of the research, that is, there is a significant and statistically significant effect of knowledge management in reducing levels of knowledge management. the crime e.

And here comes an analysis of the sub-effects of the task priorities matrix in the dimensions of knowledge in the specified time, separately at the level of the sub-hypotheses.

2-1- Analyzing the impact of knowledge management on reducing digital crime levels.

To test the validity of the third sub-hypothesis emanating from the second main hypothesis, the table ( ) shows the values of the F-test for knowledge management in reducing digital crime levels, which amounted to (313.712), and at the level of significance Sig. (2-tailed) (0.00), which means that there is a significant effect of knowledge management in reducing digital crime levels at a confidence level of 100%)), and the value of the constant ((=1.749), which means that there is a knowledge management presence of (1.749) In the directors of the Ministry of Interior under study, even if the reduction in cybercrime levels is zero, and the value of the coefficient is (0.467), meaning that increasing the value of knowledge management by one unit will lead to a change of (0.467) in reducing cybercrime levels, and the value of the coefficient of determination indicated (R2) of (0.544), which means that (54.4%) of the variance in reducing cybercrime levels is explained by the knowledge management that entered the model, and that (45.6%) is a variance explained by factors that did not enter the regression model for the study Therefore, the third sub-hypothesis is accepted within the second main hypothesis of the research, that is, there is a significant and statistically significant effect of knowledge management in reducing cybercrime levels.

And here comes an analysis of the secondary effects of knowledge management in the dimensions of reducing cybercrime levels, each separately at the level of secondary hypotheses.

Table 6.0 *A variance analysis table for the knowledge management regression equation in the dimensions of reducing digital crime levels: n = 265.*

The coefficient of determination R2 % Interpretation ratio	**Fixed limit α**	**beta regression coefficient β**	**Indication level Sig. (2-tailed)**	**F- test**	**Variables**		**Hypothesis**	
					subordinate	**independent**		
48.6%	0.926	0 .764	(0.00)	248.390	the information	knowledge management	1-3-2	Secondary
29.8%	1.813	0.476	(0.00)	83.816	electronic devices		2-3-2	
50.7%	0.879	0.740	(0.00)	270.088	persons or entities		3-3-2	

Source: The results of the statistical analysis using the statistical program spss v.28.

2-2 Analysis of the impact of knowledge management on information.

To test the validity of the first secondary hypothesis emanating from the third sub-hypothesis Table (6) shows the values of the F-test for managing knowledge in information, which amounted to (248.390), and at the level of significance Sig. (2-tailed) (0.00), which means that there is a significant effect of knowledge management on information at a confidence level of 100%)), and the value of the constant is (0.926 (=), which means that there is a knowledge management presence of (0.926) for the directorates of the Ministry under registration The study even if the information was equal to zero, and the value of the coefficient (0.764), that is, increasing the value of knowledge management by one unit will lead to a change of (0.764) in the information, and the value of the coefficient of determination (R2) of (0.486), which means that what The amount of (48.6%) of the variance in the information is a variance that is explained by the knowledge management that entered the model, and that (51.4%) is a variance explained by factors that did not enter the regression model of the current study, so the first secondary hypothesis is accepted within the third sub-hypothesis of the research, i.e. There is a significant and statistically significant effect of knowledge management on information.

3-2 Analysis of the impact of knowledge management on electronic devices.

To test the validity of the second secondary hypothesis emanating from the third sub-hypothesis Table (6) shows the values of the F-test for knowledge management in electronic devices, which amounted to (83.816), and with the level of significance Sig. (2-tailed) (0.00), and this means that there is a significant effect of knowledge management in electronic devices at a confidence level of 100%)), and the value of the constant is (1.813 (=), which means that there is a presence of knowledge management in the amount of (1.813) for the directorates of the ministry Under study, even if the electronic devices were equal to zero, and the value of the coefficient (0.476), that is, the increase in the value of knowledge management by one unit will lead to a change of (0.476) in the electronic devices, and the value of the coefficient of determination (R2) of (0.298) indicated, which It means that the amount of (29.8%) of the variance in electronic devices is explained by the knowledge management that entered the model, and that (71.2%) is a variance explained by factors that did not enter the regression model of the current study, so the second secondary hypothesis is accepted within the sub-hypothesis The third of the research, that is, there is a significant and statistically significant effect of knowledge management in electronic devices.

4-2 Analyzing the impact of knowledge management on people or entities.

To test the validity of the third secondary hypothesis emanating from the third sub-hypothesis Table (6) shows the values of the F-test for knowledge management in people or entities, which amounted to (270,088), and at the level of significance Sig. (2-tailed) (0.00), and this means that there is a significant effect of knowledge management on people or entities at a confidence level of 100%)), and the value of the constant is (0.879(=), which means that there is a presence of knowledge management in the amount of (0.879) for the directorates The ministry is under study even if the persons or entities are equal to zero, and the value of the coefficient is (0.740), that is, an increase in the value of knowledge management by one unit will lead to a change of (0.740) in the persons or entities, and the value of the coefficient of determination (R2), which is (0.507), which means that the amount of (50.7%) of the variance in people or entities is explained by the knowledge management that entered the model, and that (49.3%) is a variance explained by factors that did not enter the regression model for the current study, so accept the secondary hypothesis The third is within the third sub-hypothesis of the research, that is, there is a significant and statistically significant effect of knowledge management on people or entities.

CONCLUSIONS AND RECOMMENDATIONS

CONCLUSIONS

1-The experience of knowledge management in the departments investigated in the Ministry of Interior is weak, and this indicates administrative weakness, poor performance, and less experience available to individuals.

2-The study assumed that the application of knowledge management in the surveyed departments will contribute significantly to improving the performance of work in the surveyed departments because these departments are characterized by digital crimes and are directly with them. And the extent of its contribution to improving the performance of organizations in general.

3-The goals that the knowledge management seeks for the purpose of its application, whether it is for the interest of the security departments or for other parties, were realized by the study sample and the general tendency was the desire to apply it and its importance in the case of applying it correctly.

4-It is difficult to detect these crimes because of the lack of technical and technical expertise of individuals, and in return, the people who commit these crimes have a high level of computer skills.

5-Electronic digital crimes take a set of multiple images, and each of these images express a special problem and a special topic.

6-Electronic digital crimes are among the crimes that interfere in the country's economy, and have a direct impact on the ethics of society.

Recommendations:

1-The application of knowledge management in government organizations in general and organized crime directorates in particular has become an important and necessary matter because of its benefits to the organization, the ministry and the country in general.

2-Issuing important and appropriate laws and legislation for the purpose of enabling government organizations to practice knowledge management and apply its principles.

3-Working on developing the skills and information of working individuals and developing their ideas to give them experience and the ability to deal with the requirements of the application of knowledge management, and this by including them in training courses to develop their skills and capabilities to practice knowledge management.

4-The state should set special laws to combat digital crimes, including attacks on the privacy of individuals and organizations, and take serious steps to distance itself from the dangerous and future consequences of these crimes.

5-Amending the Terrorism Law No. 3 of 2005, which includes articles dealing with digital electronic crimes, as did the Kurdistan Region Terrorism Law No. (3) of 2006.

Sources and References

[1] Office of the High Commissioner for Human Rights, United Nations (Revealing the Massacres - Left by ISIS Terror), Report of the United Nations Mission, / November, 2018.

[2] Salah El-Din, Bou Galal (2008) (The Right to Humanitarian Assistance), Dar Al-Fikr Al-Jami, First Class, Egypt - Alexandria.

[3] Halifa, Rabah Suleiman, and Mahmoud, Kanaan Muhammad (2019) (Criminal Knowledge Management for Consumers in Electronic Commerce), Tikrit University Journal of Law Year (4), Volume (4), Number (1).

[4] Ali, Muhammad Muharram Muhammad (2003) (Scam and Electronic Commerce), a paper presented to the first scientific conference on the legal and security aspects of electronic operations) Dubai Police Academy, United Arab Emirates for the period from April 26-28.

[5] Hegazy, Abdel Fattah Bayoumi (2008) (Consumer Protection via the Internet),

House of Legal Books, Alexandria - Egypt.

[6] Article (fourteen / third / c) of the proposed Iraqi draft computer crime law for the year (2010).

[7] Article (1) of the Unified Arab Model Law for Combating Misuse of Information and Communication Technology for the year (2004).

[8] Hadi, Uday Jaber, and Muhammad, Hussein Ali (2018) (the crime of violating private life via e-mail - a comparative study), Al-Qadisiyah Journal of Law and Political Science, Al-Qadisiyah University, No. (1), Volume (1).

[9] Al-Arian, Muhammad Ali (2004) (Information Crimes), New University Publishing House, Alexandria - Egypt.

[10] Sheta, Mohamed (2001) (The idea of criminal knowledge management for computer programs), New University House, first edition, Alexandria - Egypt.

[11] Al-Malt, Ahmed Khalifa (2006) (Information Crimes), Dar Al-Fikr University, second class, Alexandria - Egypt.

[12] Salama, Muhammad Abdullah Abu Bakr (2008) (Computer and Internet Crimes), Mansha'at al-Maaref, Alexandria - Egypt.

[13] Kumar, S. (2022). A quest for sustainium (sustainability Premium): review of sustainable bonds. Academy of Accounting and Financial Studies Journal, Vol. 26, no.2, pp. 1-18

[14] Allugunti V.R (2022). A machine learning model for skin disease classification using

[15] convolution neural network. International Journal of Computing, Programming and Database Management 3(1), 141-147

[16] Tammam, Ahmed (2009) (Management of Computer Criminal Knowledge), Arab Renaissance House, Cairo - Egypt.

[17] Khalifeh, Huda (2019) (The legal and internal framework for protecting privacy on the Internet), a study published in the Journal of the Jabal Study Center, No. (26), Lebanon.

[18] Al-Janayi, Munir Muhammad, and Al-Junaihi, Mamdouh Muhammad (2005) (internet protocols and laws), Dar Al-Fikr University, first class, Alexandria - Egypt.