(IJTBM) 2023, Vol. No. 13, Issue No. IV, Oct-Dec **e-ISSN: 2231-6868 p-ISSN: 2454-468X**

Impact of Technical Distrust on Gap in Cyber Security Application Requirements According to a Standard GCI V4 2022: Survey Study in Directorate Communications and Information Systems in Iraqi Ministry of Interior

Prof. Dr. Qais Abrahim Hussain, Ameer Jasim Hussain

Universirt of Iraqia
College of Administration and Economic, Iraq

DOI:10.37648/ijtbm.v13i04.002

[1]*Received: 19 August 2023; Accepted: 01 October 2023 ; Published: 09 October 2023*

ABSTRACT

The goal of this research is the impact of the variable of suspicion and technical suspicion on cybersecurity with the effect of dimensions. For purpose of completing the scientific picture of the research, the descriptive educational approach was adopted and data was collected by means of a questionnaire, which is the research standard. The research population was (105) a sample of civilian employees, ranks, and officers in the Directorate of Communications. The information systems in the Ministry of Interior are under implementation. To choose the research hypotheses, a set of statistical methods were adopted using the outputs of the program (SPSS V25Statistician and program AMOS) this research reached conclusions, the most important of which are:

Keywords: *technical distrust; cyber security*

INTRODUCTION

Suspicion, in its origin, is considered a behavior rooted in the human psyche throughout the historical trace of the term. It is a controversial influence on all aspects of starting points and methods of thinking in all fields, especially economic and administrative, and inside and outside the organization. It is inherent to the employee working in all areas of the job and a strong influence on decision-making at all levels of management. Therefore, reputable organizations seek to discover signs of technical distrust in the organization before it occurs, especially when it comes to an activity or technical function. (N Metayer,E Jean Louis,2004:47)

THE FIRST SECTION: RESEARCH METHODOLOGY

First: The Research Problem

The process of studying, researching and analyzing employee behaviors in modern organizations constitutes one of the foundations of successful business management because it leads to reducing the circle of conflicts between employees and the organization's activities, which affects the organization's productivity and its economic and cultural returns. Therefore, the research problem is focused on trying to answer the following questions:

[1] ***How to cite the article:*** Hussain Q.A., Hussain A.J. (October 2023); Impact of Technical Distrust on Gap in Cyber Security Application Requirements According to a Standard GCI V4 2022: Survey Study in Directorate Communications and Information Systems in Iraqi Ministry of Interior; *International Journal of Transformations in Business Management*, Vol 13, Issue 4, 10-21, DOI: http://doi.org/10.37648/ijtbm.v13i04.002

The first question: What is the extent of the impact of distrust and technical distrust on decision-making regarding cybersecurity technology in the Directorate of Communications and Information Systems?

The second question: Is there an impact on the application of cybersecurity technology despite the presence of technical distrust in the Directorate of Communications and Information Systems?

Second: The Importance of Research

The importance of the research centers on the influential and effective scientific material it contains at the level of the applied aspect of the impact of technical distrust on cybersecurity technology and through the points below:

1- The study and analysis of suspicion and technical distrust in the organization identifies the mutual problems within it.

2- This research gives a new look at the behavior of technical suspicion of human resources towards the organization's activities in general and towards cybersecurity in particular.

3- Highlighting the important implications resulting from the results of technical distrust practices in a very important and young technology in the Directorate of Communications and Information Systems and the possibility of designing the results at the level of other ministries.

Third: Research Objectives

The research aims to reveal and analyze the impact of technical distrust on cybersecurity technology according to a standard(GCI V4)The sources of influence can be identified as follows:

1-Determine the impact of technical suspicious behavior on cybersecurity according to the standard (GCI V4) In light of the answers of the study sample.

-2Determining the impact of technical distrust and cybersecurity and their relationship in the Directorate of Communications and Information Systems at the Ministry of Interior is under investigation.

Fourth: The research model and its hypotheses

Figure (1) shows the research model, which shows the relationship of the influence of the independent variable and its dimensions on the variable

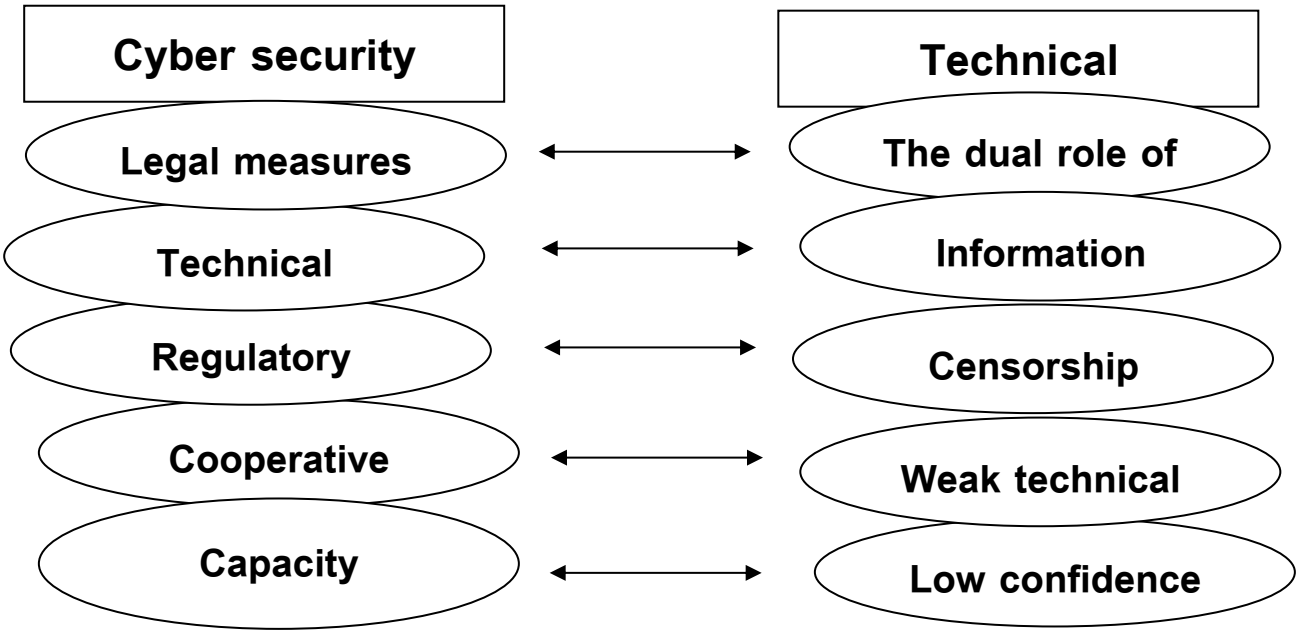


Figure No. (1) Hypothetical model for the research

Numbers of researchers

In order to achieve the research objectives and test the hypothetical model, a set of main hypotheses has been formulated as follows:

1-The main hypothesis (H):There is no significant correlation between technical distrust and the cybersecurity gap according to the requirements of the standard (GCI V4).

2-The second main hypothesis (H1: There is no significant effect of technical distrust on the cybersecurity gap according to the requirements of the standard (V4 GCI).

Fifth: Research population and sample

The researcher (Directorate of Communications and Information Systems in the Ministry of Interior) in Baghdad chose an environment for research and study, and the questionnaire was distributed to the research sample of (105) employees.

THE SECOND TOPIC: THE THEORETICAL ASPECT

First: Behaviors of technical distrust

1- The concept of technical distrust: distrust itself is an internal cognitive construct and is considered a vital and integral part of the perception of tangibles and tangibles in diagnosing things internally and externally. As for the field of business and organization sciences, distrust gives another understanding of its connection to the organization's activities and functions, as it is inversely proportional to the surrounding environment, the lower it is. The rate of distrust has increased. The rate of trust in the organization's systems, techniques, and functions, such as the cybersecurity technology under study, and the two researchers believe that the concept of suspicious behaviors of a technician represents an internal behavior that works to diagnose, analyze, and achieve dealing with decision-making requirements within the organization. ((I Ja Suntana and Others, 2023:2

2- The importance of technical distrust: Analyzing and monitoring the suspicion of employees in the organization is of great importance to senior and middle management and even subordinates, and helps them diagnose problems and conflicts in the organization and employees. Some important points can be summarized as follows:

1-The suspicious and technical behavior of employees represents an important barrier in the course of action.

2-Monitoring and controlling technical distrust increases employee confidence.

3-Low levels of technical distrust lead to increased interaction with the various technologies used in the organization.

4- Controlling the rates of technical distrust among employees in the organization leads to increasing productivity and quality and protecting the organization from external and internal threats..

J.B. McComic and others, 2023:3))

Second: Cybersecurity

1- The concept of cybersecurity: Cybersecurity means protecting the sensitive databases of every organization with the aim of repelling all hacks, attacks, and suboptimal use of data and other production processes with the aim of protecting the national economy and achieving successful management. (Showerb, Djilali, 165: 2023) It also represents the goal of enhancing the ability of countries to create and support data free of any negative effects directed towards the organization's environment at the level of closed and open networks, and to protect consistency between productive networks and modern mechanisms and technologies in order to change strong standards and balances that do not threaten Peace and economic security. (Jamal al-Din, 2023: 191)

2- The importance of cyber security: The importance of cybersecurity no longer rhymes, especially as it has become one of the sensitive necessities in our daily lives, and some points can be summarized as follows **(Al Hamada, 2705:2023)**:

a. Cyber-security represents an important and essential element in the life of the human resource inside and outside the organization.
b. 2-Cybersecurity represents the organization's first wall to protect data and production processes.
c. 4-Cybersecurity represents a young revolution in the world of modern organization and employee behavior.
d. 5-Cybersecurity enhances digital security in an organization.
e. 6-Cybersecurity improves the practices and behaviors of employees in the organization internally and externally.

3- Dimensions of cybersecurity:

a. Legal measures: The use of the Internet has led to an increase in the global digital space and a shrinkage in the social interactive space. Users of Internet engines in the world have reached 4.9 billion subscribers, representing 63% of the world's population. This leads to the emergence of electronic crime, hacking, phishing, and unauthorized use of millions of privacy. Individual and collective human resources, organizations, banks, and critical decision centers, which prompted stakeholders and decision-makers to legislate laws and regulations that regulate the use of computers and Internet engines. (Zidan, 2023: 72)
b. Technical measures: The development in cybersecurity technology that will occur is directly linked to the development of human lifestyles. As cybercrime develops, the means and methods of curbing it develop, and what a frightening competition it is, as the crime is linked to the virtual electronic awareness of Internet users, as the Cybersecurity Index explained (GCI V4) issued by the International Telecommunication Union, which announced that Egypt ranked 23rd globally out of 182 countries, while America topped 100, followed by Britain, in the field of cybersecurity support. (Saleh, 2023: 812)
c. Organizational measures: Carrying out electronic activities in a safe manner requires a secure cyberspace based on a strong foundation that curbs threats and unsafe use. This is done by building a completely closed subsystem for each organization based on economic and administrative returns

in order to achieve the organization's goals and prepare for its vision. A clear and promising message in protecting the employee and the organization at the same time. (Elham Ali Sayed Ahmed Abdullah, 2023: 7).

4- Capacity development: Many countries and organizations seek to obtain cyber sovereignty in the era of development, speed, competition, and modern automation systems, and there is no organization without cyber capabilities. Therefore, building a strong cyber bridge for any organization will bring it sustainable productivity, as is the case with the world's companies that control the market, especially the mobile phone market. Sensitive electronic software, such as iPhone and Galaxy, are two competing models.(Sharayetia, 2020: 396)

a. Information penetration: The most important factors that helped develop and support the specificities of cybersecurity digitization in organizations and employees is the emergence of the Corona pandemic and the emergence of new organizational patterns. The results were positive instead of negative due to the strong mobilizations of this transcontinental pandemic through creating a successful entrepreneurship environment and providing... An effective technical solution to support this environment, which led to the expansion, sobriety and strength of cybersecurity and a decrease in indicators of virtual penetration, phishing and unauthorized use. (Bin Zarrara et al., 2023: 60)

THE THIRD SECTION: THE APPLIED ASPECT

Firstly-Consistency Depending on the parameter values Alfakronbach

The concept of reliability in general refers to obtaining approximately the same results if the distribution of the scale is repeated again, after a certain period of time, and the Cronbach coefficient is used in this, the value of which must be greater or equal to (0.70) in order for it to be considered acceptable, as is clear from Table (1). All extracted Cronbach coefficient values are greater than the set standard and are therefore considered good, meaning that the measures used in the study have good reliability.

Schedule (1) "results Cornbrash's alpha coefficient"

the decision	Standard	Cronbach's alpha coefficient	Research variables and dimensions
Good stability	Greater or equal to 0.70	0.893	The dual role of technology
Good stability		0.889	Information hacking
Good stability		0.911	Censorship without warning
Good stability		0.896	Weak technical role
Good stability		0.908	Low confidence of workers in technology
Good stability		0.918	Technical distrust
Good stability		0.811	Legal measures
Good stability		0.823	Technical measures
Good stability		0.778	Regulatory measures
Good stability		0.795	Capacity Development
Good stability		0.9	Cooperative measures
Good stability		0.857	Cybersecurity gap according to the requirements of the specificationgci.v4

Source: Program outputsSPSS V.25

Second - Test (Half-Partition)

To further ensure that the scale used has good reliability, the researcher relied on a testHalf retail,soWhen applying this method, it was found that the coefficient(Spearman-Brown) for resolutionIt reached (0.895), while the partition coefficient was halfFor clarityUsing a parameterGuttman reached (0.891), which means that it has good stability with its various standards and can be adopted at different times.

Schedule(2)Hash testmidterm

Cronbach's Alpha	Part 1	Value	0.953
		N of Items	34
	Part 2	Value	0.932
		N of Items	34
	Total N of Items		68
Correlation between forms			0.810
Spearman-Brown Coefficient	Equal length		0.895
	Unequal length		0.895
Guttman Split-Half Coefficient			0.891

Source: program SPSS V.25

Third–Descriptive analysis of research variables

1- Technical distrust variable

The table shows (3) and shape (2) Descriptive analysis results For dimensions The technical distrust variable is as follows:

a. Overall, he achieved it **Technical distrust variable** An arithmetic mean of (3.410(at an average level and with a standard deviation) 0.614)And the coefficient of variation reached (18.01), as the availability rate of this variable reached (68.2%) As for the size of the gap, the percentage reached (31.8%)Which indicates the lack of dispersion in the sample's answers and their emphasis on the importance of the technical distrust variable, as A state of affliction among workers as a result of the negative use of technology, as they suffer from duplication in their actions and exercise undeclared supervisory roles. This is related to cases of information breaches resulting from weak technical organization, which leads to the emergence of weak points in security and a lack of trust. So Organization should be strengthened and effective policies and procedures for information security and protection against hacking should be ensured. This includes ongoing employee training on information security practices and updating systems and software to maintain a high level of security And Promoting awareness of the importance of security and preserving sensitive data. Training programs can be provided for workers on security concepts and technical risks and how to deal with them effectively.

b. The results showed that the highest overall arithmetic mean was at (Penetration Informatics) When he reached)3.470)And at the level (middle)With a standard deviation of (0.739) and a coefficient of variation of (21.3), as the availability of this dimension reached (69.4%) As for the size of the gap, the percentage reached (30.6%), as this dimension came in third place in terms of the relative importance of the dimensions **Technical distrust variable**. This indicates that This can include unauthorized access to computer systems, reading and copying personal files, or conducting electronic espionage operations. Since The impact of a cyber breach is significantly negative, as it violates individuals' privacy and exposes their sensitive information to risks. It can cause damage to personal and professional reputation, and cause harm In the directorate And business, identity theft and use in illegal activities

c. The results also showed that it was less (arithmetic mean) The total was at (**weakness The role Technical**)It reached (3.338) and at the level of (**middle**) with a standard deviation of (0.625) and a coefficient of variation of (18.72), as the percentage of availability of this dimension reached (66.8%(As for the size of the gap, the percentage reached (33.2%) This dimension came in order (**the second**) in terms of the relative importance of dimensions **a variable Technical distrust** The results indicate that There may be a lack of education and technical knowledge of individuals, which limits their ability to understand and apply Technology In solving problems, in addition to that They might be There is a lack of technical awareness of individuals, as they may

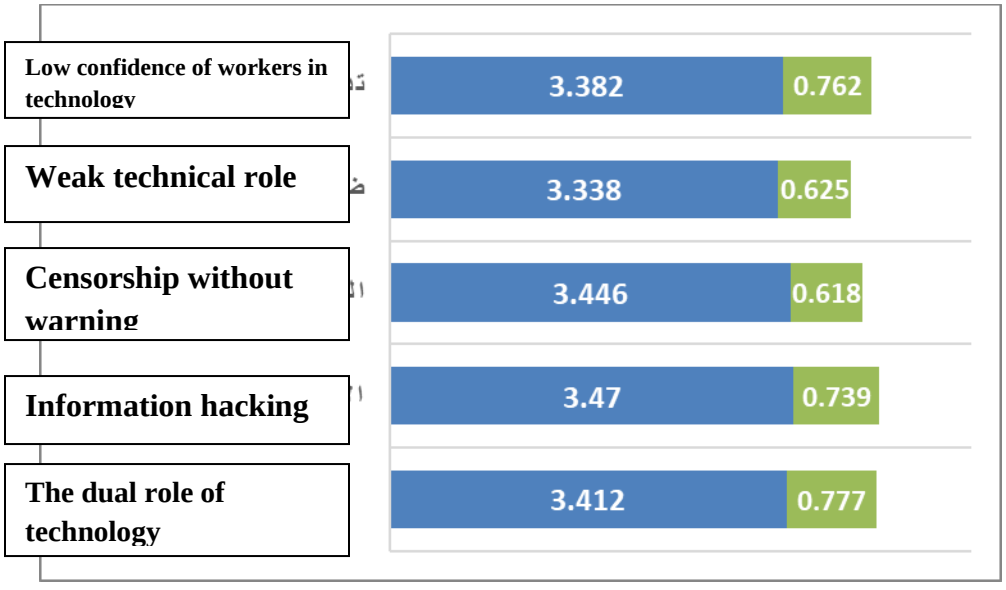
be unaware of advanced technology and its modern developments, which affects their ability to benefit from it in their daily lives. Anxiety Add to resistance Some workers To change so Some may experience anxiety or resistance to technical change, which prevents them from exploring and trying new technology applications and solutions.

d. could yet (**Censorship without former Warning**) To occupy the (first) position in terms of comparison with other dimensions of a variable **Technical distrust variable**

Schedule (3) Results of descriptive analysis of dimensions Technical distrust variable

Dimensional arrangement	**SIG**	**T**	**Disagreement rate**	**Agreement rate**	**Coefficient of variation**	**standard deviation**	**Arithmetic mean**	**Dimensions of the technical distrust variable**	**T**
5	0.878	0.154	31.8	68.2	22.77	0.777	3.412	**The dual role of technology**	1
3	0.346	0.948	30.6	69.4	21.3	0.739	3.470	**Information hacking**	2
1	0.459	0.744	31.1	68.9	17.93	0.618	3.446	**Censorship without warning**	3
2	0.323	-0.993	33.2	66.8	18.72	0.625	3.338	**Weak technical role**	4
4	0.814	-0.236	32.4	67.6	22.53	0.762	3.382	**Low confidence of workers in technology**	5
	0.876	0.156	31.8	68.2	18.01	0.614	3.410	**Technical distrust variable**	

Source: program SPSS V.25



appearance(2) The mean and deviation of the dimensions of a variable Technical distrust
Source: outputs Excel

2- A variable Cybersecurity gap according to the requirements of the specificationgci.v4

The table shows (3) and shape (2) Descriptive analysis results For dimensions Cybersecurity gap variable according to the requirements of the specificationgci.v4 As follows:

a. But overall, he achieved variable results **Cybersecurity gap according to the requirements of the specificationgci.v4**An arithmetic mean of (3.381(at an average level and with a standard deviation)0.550)And the coefficient of variation reached (16.27), as the availability rate of this variable reached (67.6%) As for the size of the gap, the percentage reached (32.4%)Which indicates the lack of dispersion in the sample's answers and their emphasis on the importance of the cybersecurity gap variable in accordance with the requirements of the specification.**gci.v4**, since gap Cybersecurity includes a set of measures to protect electronic systems, networks and data from cyber threats. Cybersecurity includes legal measures, technical measures, organizational measures, capacity development, Cooperative measures

b. The results showed that the highest overall arithmetic mean was at (**Cooperative measures**(When he reached)3.627)And at the level (**good**)With a standard deviation of (0.571) and a coefficient of variation of (15.743), as the availability of this dimension reached (72.5%) As for the size of the gap, the percentage reached (27.5%), as this dimension ranked first in terms of the relative importance of the dimensions **Cybersecurity gap variable according to the requirements of the specificationgci.v4**.

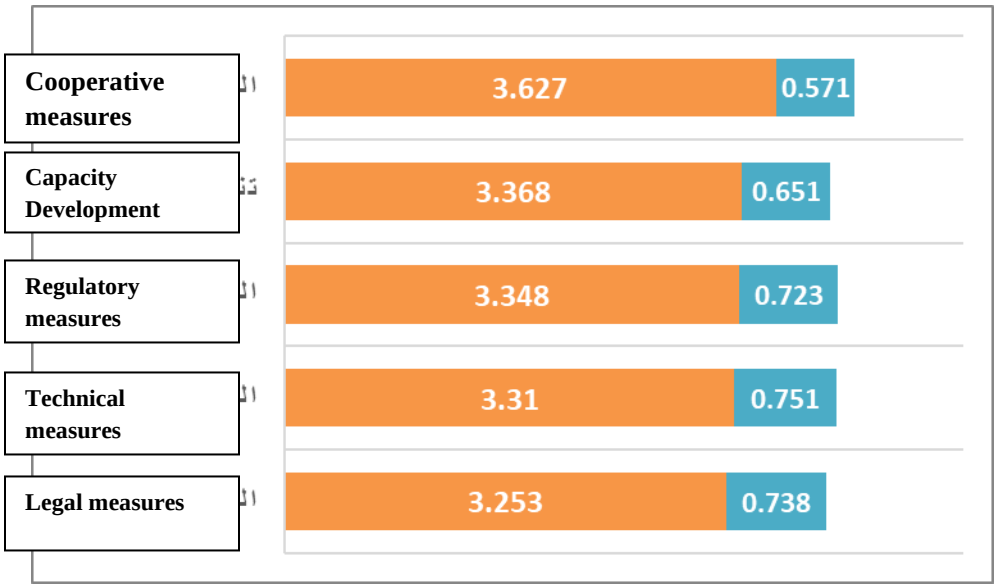
c. The results also showed that it was less(arithmetic mean) The total was at(**Legal measures**)It reached (3.253) and at the level of (**middle**) with a standard deviation of (0.738) and a coefficient of variation of (22.687), as the percentage of availability of this dimension reached (65.1%(As for the size of the gap, the percentage reached (34.9%) This dimension came in order (**the fourth**) in terms of the relative importance of dimensions **a variable Cybersecurity gap variable according to the requirements of the specificationgci.v4**

d. could yet (**Cooperative measures**) To occupy the (first) position in terms of comparison with other dimensions of a variable **Cybersecurity gap variable according to the requirements of the specificationgci.v4**.

Schedule (4) Results of descriptive analysis For dimensions Cybersecurity gap variable according to the requirements of the specificationgci.v4

Dimensional arrangement	SIG	T	Disagreement rate	Agreement rate	Coefficient of variation	standard deviation	Arithmetic mean	Dimensions of the cybersecurity gap variable according to the requirements of the specificationgci.v4	T
4	0.049	-1.995	34.9	65.1	22.687	0.738	3.253	**Legal measures**	1
5	0.234	-1.198	33.8	66.2	22.689	0.751	3.310	**Technical measures**	2
3	0.469	-0.726	33.1	67.0	21.595	0.723	3.348	**Regulatory measures**	3
2	0.626	-0.489	32.6	67.4	19.329	0.651	3.368	**Capacity Development**	4
1	0.000	3.975	27.5	72.5	15.743	0.571	3.627	**Cooperative measures**	5
	0.732	-0.343	32.4	67.6	16.27	0.550	3.381	**Cybersecurity gap variable according to the requirements of the specificationgci.v4**	

Source: programSPSS V.25



appearance(3)Mean and deviation For dimensions Cybersecurity gap variable according to the requirements of the specificationgci.v4

Source: outputs Excel

Fourthly–Testing research hypotheses

1- Hypothesis Main(first)

(nois found relationship A significant correlation what between Technical distrust and Cybersecurity gap according to the requirements of the specificationgci.v4)

reach Factor Link between **Technical distrust And Cybersecurity gap according to the requirements of the specificationgci.v4** (0.820) when level indication(0.000)It is less than the significance level (0.05).,When the value reached (Z(calculated)11.393) It is greater than the value (Z(Extreme tabulation)1.96This result indicates the significance of the correlation value, as it was at a strong level, and this Means Acceptance Alternative hypothesis Which states on(There are **relationship Engagement Self indication moral between Technical distrust And Cyber-security gap according to the requirements of the specificationgci.v4**)

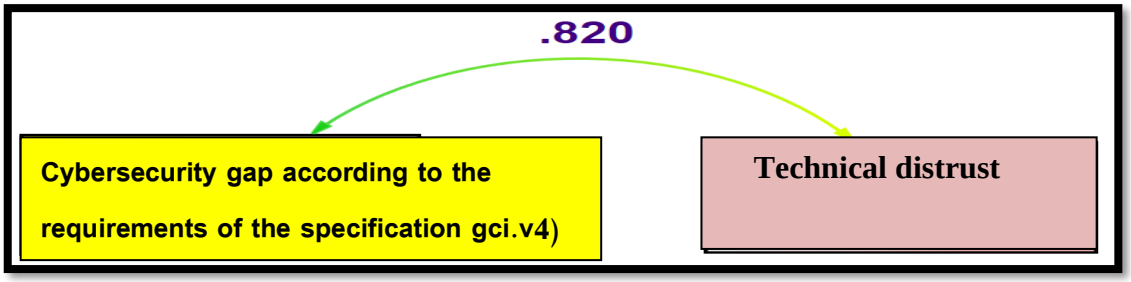


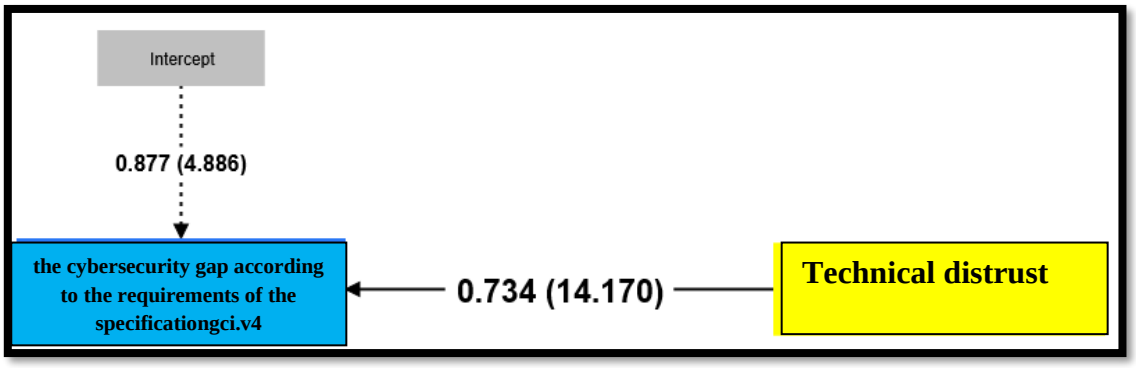
Figure (4) values of the correlation between the dimensions of technical distrust and the cybersecurity gap according to the requirements of the specificationgci.v4

Source: Program outputsAmosV.25

2 -Main hypothesis(the second)

(nothing impact Dhu indication Moral Technical distrustin Cybersecurity gap according to the requirements of the specificationgci.v4)
Cybersecurity gap according to the requirements of the specificationgci.v4 = 0.877+ 0.734 (technical distrust)

The table shows (4) and shape (4) Results of the impact analysis between **Technical distrust in the cybersecurity gap according to the requirements of the specificationgci.v4**, since I achieved (F) The extracted value is (200.785), indicating this result There is a significant effect between them, as shown by the value of (t) extracted (14.170) indicates that the effect of the parameter (β) is a real effect, as increasing the effect by one unit will lead to an increase in the cybersecurity gap according to the requirements of the gci.v4 specification by (73%), as the size of the effect reached (1.417) which is at a (large) level, as the technical distrust variable was able to explain the percentage (66%) of the changes that occur in the cybersecurity gap according to the requirements of the specification**gci.v4**. In light of what has been presented MWe accept the alternative hypothesis and reject the null hypothesis (There is a significant effect For a variable Technical distrustin Cybersecurity gap according to the requirements of the specificationgci.v4)



appearance (5) Analyzing the impact of technical distrust on the cybersecurity gap according to the requirements of the specificationgci.v4

Schedule (5) Analyzing the impact of the dimensions of technical distrust on the cybersecurity gap according to the requirements of the specificationgci.v4

the decision	Sig	The strength of the impact	Effect size	(Z)	(t)	(F)	(R2)Adj	(R2)	(R)	Dimensions of the technical distrust variable			Dependent variable
Accept the alternative hypothesis	0.000	big	1.2678	10.500	12.678	160.737	0.617	0.621	0.788	1.477	(α)	The dual role of technology	Cybersecurity gap according to the requirements of the specificationgci.v4
										0.558	(β)		
Accept the alternative hypothesis	0.000	big	1.0723	9.253	10.723	114.979	0.535	0.540	0.735	1.482	(α)	Information hacking	
										0.547	(β)		
Accept the alternative hypothesis	0.000	big	0.9029	8.057	9.029	81.530	0.449	0.454	0.674	1.314	(α)	Censorship without warning	
										0.600	(β)		
Accept the alternative hypothesis	0.000	big	0.9757	8.581	9.757	95.203	0.488	0.493	0.702	1.317	(α)	Weak technical role	
										0.618	(β)		
Accept the alternative hypothesis	0.000	big	0.882	7.896	8.820	77.796	0.437	0.443	0.665	1.757	(α)	Low confidence of workers in technology	
										0.480	(β)		
Accept the alternative hypothesis	0.000	big	1.417	11.393	14.170	200.785	0.669	0.672	0.820	0.877	(α)	Technical distrust	
										0.734	(β)		

SECTION FOUR: CONCLUSIONS AND RECOMMENDATIONS

First: conclusions

This part is devoted to presenting the most important conclusions derived from the applied aspect, which are as follows:

1- The results of the research in the directorate, the research sample, showed the impact of technical distrust on the cybersecurity gap. This is an indication of employees' interaction with cybersecurity technology in isolation from some barriers related to developing their capabilities and skills, information penetration, and some technical measures.

2- Cybersecurity technology for employees inside and outside the organization represents a barrier against virtual intrusions, which increases the technical suspicion index.

3- It is possible to support and develop cybersecurity technology because it achieves the improvement of the productivity quality index if it is placed in a closed circle and kept pace with the rapid development under the global umbrella.

Second: Recommendations

Through the conclusions reached, the researchers recommend the following to the Directorate of Communications and Information Systems in the Iraqi Ministry of Interior:

1- Paying attention to early monitoring of indicators of technical distrust among employees working in the organization.

2- Providing a special section for training and qualification exclusively in the field of cybersecurity, within a closed space, and closed virtually and administratively in order to raise the skill and efficiency levels of employees.

3- Providing universities and institutes with specialization in cybersecurity at the graduate and professional levels so that it becomes a prevalent culture like the culture of first aid.

RESOURCES

1. Bin Zurara, Amina, Bedouin, & Fatima. (2023). Innovative digital solutions in the field of identity protection, privacy and cybersecurity during the Covid-19 pandemic. Digitization Journal for Media and Communication Studies, 3(1), 58-66.
2. Conditions. (2020). Cyber sovereignty in China between power requirements and national security necessities.
3. Dr.. Elham Ali Sayed Ahmed Abdullah. (2023). A comprehensive literature review: revealing the differences and intersections between information security and cybersecurity: Dr. Elham Ali Sayed Ahmed Abdullah. Journal of the Arabian Peninsula Center for Educational and Humanitarian Research, 1(2), 1-21.
4. Dr.. Musaad Abdul Rahman Zidan Qasim Zidan. (2023). Cybercrimes and their effects on societal security in light of public international law.
5. Jamal Al-Din, H. (2023). Cybersecurity and transformation in the international system. Journal of the Faculty of Economics and Political Science, 24(1), 189-230.
6. McCormick, J. B., Hopkins, M., Lehman, E. B., & Green, M. J. (2023). Political views and organizational distrust affect rural residents' willingness to share personal data for COVID-19 contact tracing: A cross-sectional survey study. Journal of Clinical and Translational Science, 7(1), e91.
7. Metayer, N., Jean-Louis, E., & Madison, A. (2004). Overcoming Historical and Institutional Distrust. Ethnicity & Disease, 14, 46-52.
8. Xue, J., Deng, Z., Wu, T., & Chen, Z. (2023). Patient distrust toward doctors in online health communities: integrating distrust construct model and social-technical systems theory. Information Technology & People, 36(4), 1414-1438.