Al-Qadisiyah Journal for Administrative and Economic Sciences ISSN$_{Online}$: 2312-9883
QJAE, Volume 24, Issue 3 (2022) ISSN$_{Print}$: 1816-9171
Manuscript ID:

The effect of continuous improvement in the quality of cybersecurity by mediating customer orientation

Amir Sajit Mdlool[1] Prof Dr. Aseel Ali Mezher[2]

[1] University of Al-Qadisiyah / College of Administration and Economics / Business Administration Department(Admin.mang21.11@qu.edu.iq)

[2] University of Al-Qadisiyah / College of Administration and Economics / Business Administration Department(aseel.mezher@qu.edu.iq)

*Corresponding Author Amir Sajit Mdlool Affiliation:*University of Al-Qadisiyah
Email Admin.mang21.11@qu.edu.iq

Abstract

The current study aimed to shed light on the impact of continuous improvement in enhancing the quality of cybersecurity by mediating customer orientation, as continuous improvement indicates that it is an organized process at the organization level that aims to eliminate all types of waste in all processes or systems. It includes four dimensions (plan, do, check, and correct), while the quality of cyber security can be expressed as a set of activities, practices and tools that can be used to protect the cyber environment from unauthorized (illegal) access and/or use of information. It includes seven dimensions (knowledge of system security, electronic attacks, access to the system, weaknesses, potential damage, timely detection of the attack, and the restoration of the system after penetration), while the orientation towards the customer is defined as the vision and objectives of the organization or the sum of the values and beliefs that it adopts. An organization that puts the customer among its priorities. It includes two dimensions (need and pleasure), and the current study focused on the internal customer. For this purpose, the questionnaire was adopted as a basic measuring tool for collecting data from the sample under study, which amounted to (150) questionnaires distributed to (150) members of the Cyber Security Department in the Iraqi National Security Service, and the percentage of questionnaires valid for analysis was (141) questionnaires. A set of ready-made computer programs (SPSS vr.24 and AMOS vr.24) were employed to test the main and sub-study hypotheses. The study reached a set of conclusions, the most prominent of which was the existence of a direct and indirect correlation and impact between the study variables (continuous improvement, quality of cybersecurity, and orientation towards customer), and that continuous improvement processes are an essential factor in modern and successful organizations. Thus, continuous improvement processes have an important role in the National Security Agency / Cyber Security Department.

Keywords: continuous improvement, quality of cyber security, customer orientation Key words: continuous improvement, cyber security, customer orientation

المستخلص

هدفت الدراسة الحالية إلى تسليط الضوء على تأثير التحسين المستمر في تعزيز جودة الامن السيبراني بتوسيط التوجه نحو الزبون، اذ يشير التحسين المستمر الى انه عملية منظمه على مستوى المنظمة تهدف إلى القضاء على جميع انواع الهدر في جميع العمليات أو الأنظمة. ويتضمن اربعه ابعاد هي (خطط، اعمل، افحص، وصحيح)، أما جودة الامن السيبراني فيمكن التعبير عنها بانها مجموعه من الأنشطة والممارسات والأدوات التي يمكن استخدامها لحماية البيئة السيبرانيه من الوصول و/او الاستخدام غير المصرح به (غير القانوني) للمعلومات. وتضم في طياتها سبعة ابعاد هي (المعرفة بأمن النظام، الهجمات الإلكترونية، الوصول للنظام، نقاط الضعف، الضرر المحتمل، اكتشاف الهجوم بالوقت المناسب، واستعادة النظام بعد اختراقه)، في حين يُعرف التوجه نحو الزبون بانه رؤية وأهداف المنظمة او مجموع القيم والمعتقدات التي تتبناها المنظمة والتي تضع الزبون ضمن اولوياتها. ويتضمن بُعدين هما (الحاجة والمتعة)، وقد ركزت

الدراسة الحالية على الزبون الداخلي. وقد تبنت من اجل ذلك الاستبانة كأداة قياس أساسية لجمع البيانات من العينه محل الدراسة والتي بلغت (150) استبانة وزعت على (150) منتسب تقريباً من قسم الامن السيبراني في جهاز الامن الوطني العراقي، وكانت نسبة الاستبانات الصالحة للتحليل (141) استبانه. وقد وظفت لاختبار فرضيات الدراسة الرئيسة والفرعية مجموعه من البرامج الحاسوبيه الجاهزة وهي (SPSS vr.24) و (AMOS vr.24)وتوصلت الدراسة إلى مجموعة من الاستنتاجات كان من أبرزها وجود علاقة ارتباط وتأثير مباشر وغير مباشر بين متغيرات الدراسه (التحسين المستمر وجودة الامن السيبراني والتوجه نحو الزبون)، وان عمليات التحسين المستمر تعد عامل اساسي في المنظمات الحديثة والناجحة. وبذلك فأن لعمليات التحسين المستمر دور مهم في جهاز الامن الوطني / قسم الامن السيبراني.

الكلمات المفتاحيه: التحسين المستمر، جودة الامن السيبراني، التوجه نحو الزبون

introduction

Continuous improvement is a comprehensive scientific method, the main objective of which is to improve the performance of the organization and thus improve the quality of products or services. Continuous improvement is an organized process at the organization level that aims to eliminate all types of waste in all processes or systems and exclude everything that does not add value to the organization and enhance its ability to survive for leadership and excellence to achieve customer desires and expectations.

In light of the great digital transformation, organizations have turned to the era of digitization to achieve their goals. The use of new technologies may improve efficiency and security but also increase cyber risks. In order to realize and fully embrace the benefits, cybersecurity must be considered at all levels of the organization, and organizations need to create and follow a robust cyber strategy. A large part of security breaches are caused by bad people and processes, which means that the physical aspects related to technological security systems must also be taken into account when assessing cyber risks. authorized (unlawful) information.

Nowadays, customer expectations and behavior must be taken into consideration not only in the downstream stages, but along the processes needed to deliver value-added products and services. Customer orientation as a strategic orientation reflects the organization's ability to create and deliver superior value to customers by processing market information. Orientation towards the customer is defined as referring to the vision and objectives of the organization or the sum of the values and beliefs that the organization adopts and which put the customer among its priorities.

According to the foregoing, the current study attempts to stand on the level of cyber security quality in the Iraqi National Security Service / Cyber Security Department. This study also attempts to clarify the importance and role of cyber security, as well as clarify the nature, and type of relationship between the dimensions of continuous improvement, the quality of cyber security and customer orientation. For the purpose of taking note of what was mentioned above, the study was divided into four chapters, the first chapter of which was devoted to presenting the study's methodology (the problem of the study, its objectives, importance, limits, hypotheses and a description of its sample, as well as the most important means and moral tools with the aim of testing its hypotheses), and the second section dealt with some of the previous relevant cognitive efforts with its variables. As for the second chapter, it dealt with the theoretical aspect of the study, and it was divided into four sections, the first of which was devoted to providing a theoretical framing about the concept, and the removal of continuous improvement, while the second section dealt with the concept and the removal of the quality of cybersecurity and presenting the views of some researchers on this concept, while the third topic has The concept and dimensions of customer orientation, while the fourth topic presented the relationship between the study variables. The third chapter of the study was devoted to the practical side, which included three sections. The first section dealt with testing the study's standards and building its model and verifying the validity and reliability of the measurement tools adopted in this study. The second topic was devoted to providing a presentation and analysis of the level and importance of the study variables by addressing the opinions of the two researchers that revealed their answers to the paragraphs of the study tool, while the third section dealt with testing and analyzing the hypotheses of correlation and influence relationships, while the last chapter of the study focused on the fourth chapter. Which was devoted to presenting a set of conclusions reached by the study and a number of recommendations and

proposals for future studies that the current study hopes will contribute to solving the problem of Study, and to take its way of interest by researchers and scholars.

Methodology

First: the problem of the study

Continuous improvement is a comprehensive scientific method, the main objective of which is to improve the performance of the organization and thus improve the quality of products or services. In the era of globalization and electronic openness based on knowledge and informatics through the international information network (Internet), countries, governmental organizations and individuals alike have become more dependent on information systems and more use of devices connected to the Internet from mobile phones, personal computers, and tablets. The number of people connected to the cyberspace, which has increased with it cyber-attacks and information security breaches, and cybersecurity challenges resulting from widening security gaps, which criminal groups and individuals use to achieve criminal goals aimed at disturbing public order or obtaining personal gains, which poses a threat to security at the level of Individuals, what necessitates raising cyber awareness among members of the Iraqi society, and the fact that the Cyber Security Department in the Iraqi National Security Service is the first concerned with the subject, he must realize the importance of cyber security. And work to ensure the rights of individuals and keep them away from all risks and damages resulting from hacking their accounts, electronic attacks and other matters related to that. Nowadays, customer expectations and behavior must be taken into consideration not only in the downstream, but along the processes needed to deliver value-added products and services. Orientation to the internal customer as a strategic orientation reflects the organization's ability to create and deliver superior value to internal customers by addressing market information.

The main research problem is represented by the following question: Is there an effect of continuous improvement in the quality of cybersecurity through customer orientation? Several sub-questions arise from this question, including:

1- What is the level of continuous improvement in the cybersecurity department?

2- To what extent are employees in the cyber security department aware of the importance of cyber security?

3- Is there a direct impact of continuous improvement in the level of quality of cybersecurity?
4- What is the nature of improvement required to increase the quality of cybersecurity?

Second: the importance of the study

The importance of the study stems from the importance of the variables investigated (continuous improvement, quality of cybersecurity, and orientation towards the customer), as it is one of the important topics that have received the attention of a large number of researchers. Continuous improvement at the present time is an important phenomenon.

To deal with it with great care and seriousness, especially if it is directed towards the internal customer and in accordance with his needs and ensures his enjoyment in that.

Third: Objectives of the study

1. Identify the nature and level of continuous improvement in the Cyber Security Department.

2. Getting acquainted with the reality and level of the security services provided in the Cyber Security Department.

3. Provide a comprehensive picture of the current cybersecurity trends by identifying the areas for improvement required in accordance with the requirements of the internal customer.

4. Determining the level of security services provided by the Cyber Security Department of the Iraqi National Security Agency to the internal customer (from the officers and ranks) from the point of view of the service providers.

Fourth: Data and information collection tools

For the purpose of completing the requirements of completing the theoretical aspect of the study, it relied on Arab and foreign references such as books, studies, letters, scientific thesis, publications, periodicals and research related to the study, as well as making use of the international information network (Internet). In its practical aspect, the study relied on two aspects, the first being personal interviews with officers and employees of the Cyber Security Department. As for the second aspect, the questionnaire forms were adopted as a main tool for collecting data and information related to the variables of the study, and it used the five-point Likert gradient (Likert) being the most common and used in the administrative and social sciences. This form included a number of axes.

fifth: The scheme of the hypothetical study

In light of the study's methodology and objectives, a hypothetical study plan was prepared, see Figure (1), to express the relationship between the study variables.

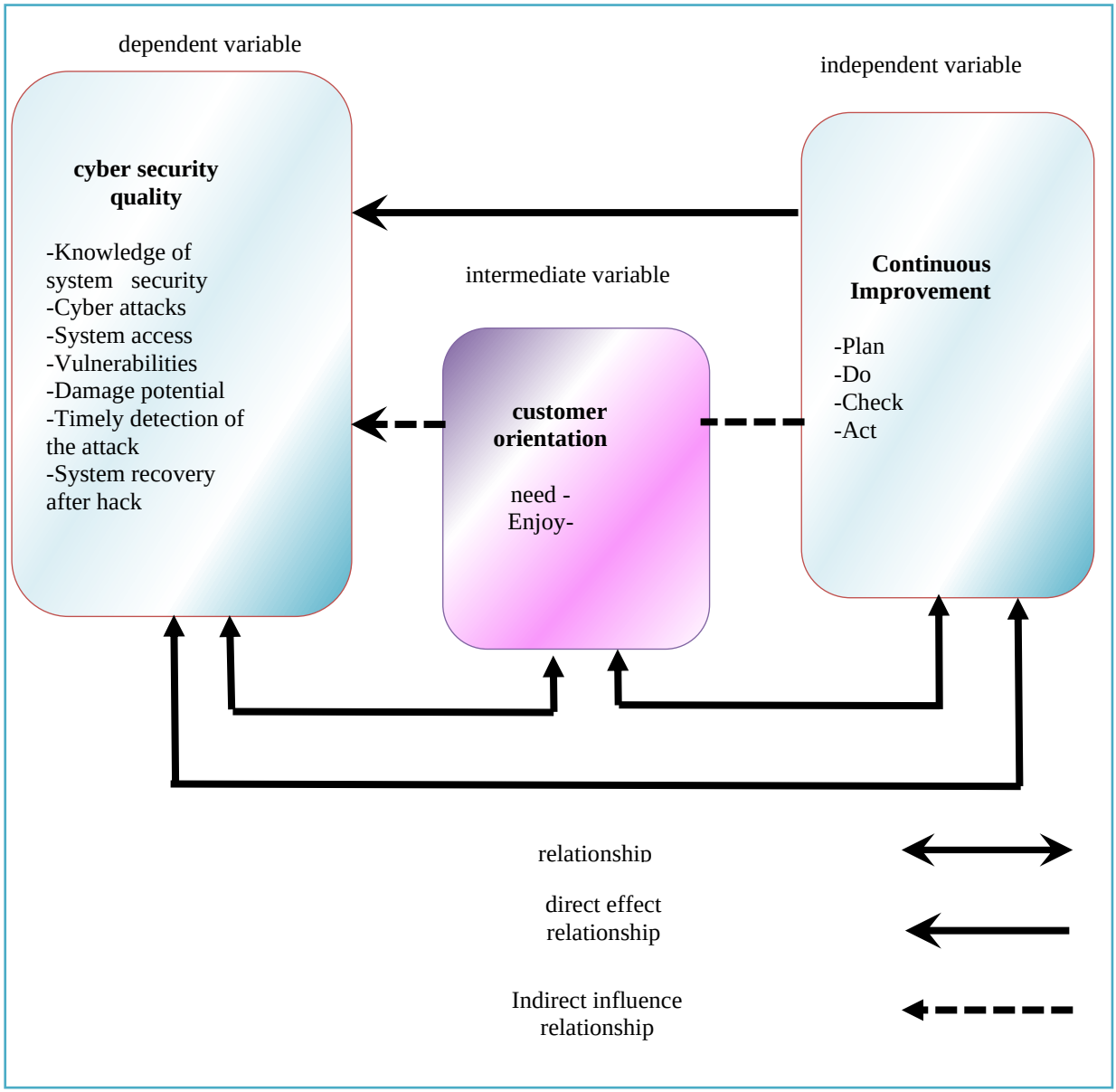

Figure (1) theoretical framework for research

Sixth: The hypotheses of the study

Based on the hypothetical scheme developed by the current study, the following hypotheses can be formulated:

A: Correlation hypotheses

1- There is a significant correlation between continuous improvement and customer orientation. The following sub-hypotheses emerge from this hypothesis:

•There is a significant correlation between plans and orientation towards the customer in its individual or combined dimensions.

•There is a significant correlation between the action and orientation towards the customer in its individual or combined dimensions

•There is a significant correlation between the check and the orientation towards the customer with its dimensions, individually or collectively.

•There is a significant correlation between Actness and orientation towards the customer with its dimensions, individually or collectively.

2- There is a significant correlation between continuous improvement and the quality of cybersecurity. The following sub-hypotheses emerge from this hypothesis:

•There is a significant correlation between plans and the quality of cybersecurity with its dimensions, individually or collectively.

•There is a significant correlation between action and the quality of cybersecurity with its dimensions, individually or collectively.

•There is a significant correlation between check and the quality of cyber security with its dimensions, individually or collectively.

•There is a significant correlation relationship between authenticity and the quality of cybersecurity with its dimensions, individually or collectively

3- There is a significant correlation between customer orientation and cybersecurity quality. The following sub-hypotheses emerge from this hypothesis:

•There is a significant correlation between the need and the quality of cybersecurity in its dimensions, individually or collectively.

•There is a significant correlation between fun and the quality of cybersecurity in its dimensions, individually or in combination.

B: direct and indirect influence hypotheses

1- There is a significant effect between continuous improvement and customer orientation. The following sub-hypotheses emerge from this hypothesis:

•There is a significant effect between the plans, and the orientation towards the customer with its dimensions, singly or collectively.

•There is a significant effect between the action and the orientation towards the customer in its singular or combined dimensions

• There is a significant effect between the check and the customer orientation with its dimensions, singly or in combination.

• There is a significant effect between Actness and orientation towards the customer in its individual or combined dimensions.

2- There is a direct and significant effect between continuous improvement and the quality of cybersecurity. The following sub-hypotheses emerge from this hypothesis:

• There is a direct effect with a moral significance between plans and the quality of cybersecurity in its dimensions, individually or in combination.

• There is a direct effect with a moral significance between the action and the quality of cybersecurity with its dimensions, individually or in combination.

• There is a direct and significant effect between check and the quality of cybersecurity in its dimensions, individually or in combination.

• There is a direct effect with a moral significance between the Actness and the quality of cybersecurity in its dimensions, individually or in combination

3- There is a significant effect between customer orientation and cybersecurity quality. The following sub-hypotheses emerge from this hypothesis:

• There is a significant effect between the need and the quality of cybersecurity in its dimensions, individually or in combination.

• There is a significant effect between the fun and the quality of cybersecurity in its dimensions, individually or in combination.

4- There is an indirect effect with a moral significance between continuous improvement in its individual or collective dimensions and the quality of cyber security in its individual or collective dimensions through an orientation towards the customer in its individual or collective dimensions.

Seventh: The study community and its sample

The study population was represented by the Cyber Security Department of the Iraqi National Security Service. The study sample consisted of all the affiliates in the Cyber Security Department of the Iraqi National Security Service, who numbered approximately (150 members), as the number of questionnaire forms distributed to the study sample was (150), of which were adopted (141) Forms only for their validity for analysis and leaving the rest either because they were not returned or because there is a shortage in them, meaning that the recovery rate reached 94%,

Axis: the theoretical side

First, the concept of continuous improvement

Continuous improvement means an increased and continuous effort to improve products, processes and services. Continual improvement should be seen as a process "to achieve improvement" rather than as a series of isolated improvement activities, and continuous improvement is described as a process within more comprehensive quality improvement strategies (Meiling et al., 2012:141). Continuous improvement is nowadays an important phenomenon very he is A vital component in achieving business excellence Continuous improvement emerged in Japan in the sense of kaizen after World War II. The word kaizen means "continuous improvement" and is a system used in quality, technology, operations, organizational culture, productivity, safety and leadership, and is derived from the Japanese words (Kai, which means "Change" or "Action" and (Zen) which means good, and kaizen at the organizational level is oriented towards the organizations themselves and extends to the personal and social life of the individual (Charantimath, 2017:183). Here (Erdur, 2019:5) is known as a continuous improvement program Broad, planned, organized, and systematic change distinct from project-based change models. It is also defined (Lizarelli et al., 2021:3) as a culture that aims to eliminate waste in all systems and processes, including all individuals involved in relevant entities.

Second, the dimensions of continuous improvement

The dimensions of continuous improvement obtained almost unanimously by most of the book are known as the Deming cycle:

1- **Plans**: In this stage, the principle and goal are defined and a plan is developed (Shyng, 2021:208).

2- **Do**: The purpose of this stage is to implement the Action Plan (Chakraborty, 2016:16))

A - Implementation of improvement.

b- Collecting and documenting data.

C - Documenting problems, unexpected observations, lessons learned, and acquired knowledge.

3- **Check**: At this stage, the effectiveness of the updated process is checked, and gaps are identified in the updated process (Arias, 2020:4)

4- **Act**: It is the stage in which the process is improved with problem-solving in the specific, recorded process from the two stages (act and check) and investigation of the root causes of problems if any,

and eliminating them by modifying the process. The test repeats to collect new data and reassess; Or abandon the project and start over again (Silva et al., 2017:325).

Third: The importance of continuous improvement

The importance of continuous improvement in the business environment stems from three main phenomena: - Changes in the business environment, the emergence of new management systems, and the importance of quality management itself. Organizations must focus on eliminating waste and identifying new areas of improvement (Sanchez & Blanco, 2014:2). Whereas (Soita, 2016:14) finds that the importance of continuous improvement lies in preventing waste that includes wastage of time, costs, lack of use of Act thinking, or other resources that were spent in producing a product or service.

Fourth: Continuous Improvement Objectives

Lizarelli et al., 2021:3) believes that the overall goal of continuous improvement is to focus on reducing waste and eliminating activities that do not add value to the operations. The goal can be to reduce waste, improved quality, and an efficient production line Among many other objectives and by using the many characteristics of CI, it can be used to solve problems based on production and processes and also to help organizations grow in the world of organizations. (Ritamaki, 2017:19)

Fifthly: The quality of cyber security

In the American Society for Quality Control (ASQC), the American Society for Quality Control (ASQC) has given a formal definition of quality as: "The sum of features and characteristics of a product or service that affect its ability to meet certain needs" (Vlad, 2019:17). Juran (1951), who is one of the main and important figures in the process of defining quality and quality management, identified two main meanings of quality: - the features of products that meet the needs of customers and thus provide their satisfaction as well as freedom from deficiencies and freedom from errors (Marouni, 2017:10)). Teoh & Mahmood, 2017:1) goes on to say that cybersecurity is a critical component at the national level as countries need to balance the needs of digital economies and ensure the reliability and security of cyberspace. Protection from cyber threats has become a top priority for countries around the world. While (Brodin, 2019:1) indicates that cybersecurity is a matter related to national security, and therefore it needs to be dealt with as a matter related to national security, as contemporary cybersecurity challenges pose a great danger to it, and therefore the examination of this field generates theoretical and social importance, Through process tracking method. (Düveroğlu, 2020:44) defines cyber security as protecting computer systems from theft or damage to their hardware, software or databases, and even from disruption of operations and services, they provide to society.

Sixth: Dimensions of the quality of cybersecurity

1- Knowledge of security The first security dimension of the control system is knowledge of the security of the system through the security group, as the security group represents those people in your organization who are directly responsible for the security of control systems. Security risks are closely related to knowing the security of your system. (Boyer & Queen, 2008:2)

2- Cyber-attacks: the use of a deliberate action to alter, disable, deceive, weaken or destroy hostile computer systems or networks, or information and/or software contained within or passing through such systems or networks, (Pipyros *et al*., 2018:5).

3- Access: The design, configuration, or deployment features of a system that provide a potential attacker with the ability to send or receive data to/from a component of the control system from the attacker's location (Boyer & Queen, 2008:2)

4- Vulnerabilities: They are flaws in the system that are likely to be exploited by malicious parties. (Bothur et al., 2017:82)

4- Potential damage: The potential to exploit weaknesses and cause losses. (Lamba et al., 2015:5834)

6- Timely attack detection: In recent years, the number of attacks on networks has increased significantly, and with it the interest in discovering electronic attacks has increased among researchers (Singh & Silakari, 2009:1).

7- Restoring the system after its breach is to provide quick recovery to electronic communication networks, information systems, or control systems in the event of electronic accidents or electronic attacks. (Limba et al., 2019: 560) Seventh: Cybersecurity Objectives

Mishra, 2020 sees that the goals of cyber security lie in avoiding cyber failures that involve high costs, including financial risks arising from data breaches, strategic risks to critical infrastructure, and, in the extreme, loss of life and money.

Eighth: The importance of cyber security

Veale & Brown,2020:1)) expressed the importance of cyber security by saying (The importance of cyber security has increased with the movement of many governments, commercial and daily activities around the world online. But especially in emerging economies, "any organizations that are digitizing lack (Hawamleh et al., 2020:3) bebelievehat cybersecurity ensures that the organization achieves and maintains its security characteristics and user assets against Security risks within the cyber environment.

Ninth, customer orientation

Customer orientation is a business philosophy or policy statement that aims to meet needs and is a long-term method for building relationships with customers from a point of view. What the organization practices and what the customer values (Duffy et al., 2020:2). In fact, the growing concerns in customer orientation, rapid advances in technology, increased competition, and globalization have led to the modification of the role of the customer. (Aburayya et al., 2020:2148) Customer orientation (Paul, 2020:2) is defined as an adequate understanding of target customers. In order to continuously create higher value for them.

Tenth: The dimensions of customer orientation

1- Need: It refers to the employees' beliefs about their ability to meet the needs of customers (He *et al*., 2015).

2- Pleasure: The pleasure dimension is related to the fact that workers can enjoy the interaction and serve the needs of their customers (Aburayya et al., 2020:2149).

Eleventh: The importance of customer orientation

(Lee *et al*., 2021:4) emphasized that customer orientation as external stakeholders has a significant impact on organizational social sustainability, through Providing valuable insights into the external environment. (KANG *et al*., 2021:39) asserts that with the intensification of competition between organizations and the increase in customer influence, customer-oriented marketing has become more important, as the customer-oriented attitude increases their satisfaction and improves business performance. (Muzumdar & Kurian, 2021:43) believes that customer orientation improves the salesperson's ability to listen, thus indirectly affecting customer loyalty in the form of buyback.

third axis: the practical side

First, coding and characterization

Analyzing the data easily and with high credibility, and extracting accurate results requires expressing them with a set of symbols that facilitate the statistical analysis of the data included in the analysis, and Table (1) shows the description and symbolization of the variables and dimensions of the current study.

Table (1)

Coding and characterization of the study variables

T	The main variables	sub-variable	number of paragraphs	code
1	continuous improvemen t	plan	5	PL
		Do	5	DO
		check	5	CH
		Act	5	AC
2	cyber security quality	Knowledge of systemm security and management	5	KSS
		cyber attacks	5	CYA
		System access	4	SYA
		Vulnerabilities	4	VUI
		Damage potential	4	DAP
		Timely detection of the attack	3	TDA
		System recovery after hack	4	SRH
3	customer orientation	enjoy	6	EN
		need	6	NE

Source: Prepared by the researcher

Second, confirmatory factor analysis

1- Results of the axis of continuous improvement

Through the use of confirmatory factor analysis and based on the statistical program Amos vr.24, the study worked here to build a structural model for the dimensions and paragraphs of the axis of continuous improvement. The acceptance of the model is judged by observing the values of the criteria that were previously explained, in addition to that, the participation rates for each of the paragraphs are determined. Dimensions in the interpretation of that axis. Here, the dimensions of the continuous improvement axis will be addressed. For the purpose of testing the constructivist model for the confirmatory factor analysis for this axis, a set of criteria were extracted related to the dimensions of the continuous improvement axis and were placed in Table (2):

Table (2)

Criteria for appropriateness of the model and the decision of the current study

used standard	X^2 (sig)	GFI	IFI	RMSE A
Standar d value	366.825 (0.000)	0.81	0.84	0.00

Acceptance limits	5% min	0.50 max	0.50 max	0.08 min
the decision	Fitting Form	Fitting Form	Fitting Form	Fitting Form
Standard value	366.825 (0.000)	0.81	0.84	0.00

Source: Prepared by the researcher based on the results of the program Amos vr.24

It is clear from the above table that the model used by the current study is an appropriate model based on the values of the criteria, as this result leads us to the conclusion that the possibility of adopting this model is that the criteria have achieved their assumed limits. From it it is clear that the paragraphs of the dimensions of the (continuous improvement) axis have participated in the interpretation of the axis in different proportions based on their estimated values.

2- Results of the quality of the cybersecurity axis

Through the use of confirmatory factor analysis, and based on the statistical program Amos vr.24, the study worked here to build a structural model for the dimensions and paragraphs of the cybersecurity quality axis. Paragraphs dimensions in the interpretation of that axis. For the purpose of testing the structural model for the confirmatory factor analysis of the cybersecurity quality axis, a set of criteria were extracted related to the paragraphs of the dimensions of this axis, which are presented in Table (3)

Table (3)

Criteria for appropriateness of the model and the decision of the current study

used standard	X^2 (sig)	GFI	IFI	RMSEA
Standard value	515.487 (0.000)	0.81	0.86	0.00
Acceptance limits	min 5%	max 0.50	max 0.50	min 0.08
The decision	Fitting Form	Fitting Form	Fitting Form	Fitting Form

Source: Prepared by the researcher based on the results of the program Amos vr.24

It is clear from Table (3) that the model used by the study is an appropriate model based on the criteria values. As this result leads us to the conclusion that the possibility of adopting this model because the standards have achieved their supposed limits. From it it is clear that the paragraphs of the dimensions of the quality of cyber security axis have participated in the interpretation of this axis in different proportions based on their estimated values.

3- Results of the customer orientation axis

For the purpose of testing the constructivist model of the confirmatory factor analysis for this axis, a set of criteria was extracted related to the paragraphs of the dimensions of the axis of customer orientation, which are presented in Table (4)

Table (4)

Criteria for appropriateness of the model and the decision of the current study

used standard	X^2 (sig)	GFI	IFI	RMSEA
Standard value	84.878 (0.000)	0.89	0.83	0.00
Acceptance limits	5% min	0.50 max	0.50 max	0.08 min
the decision	Fitting Form	Fitting Form	Fitting Form	Fitting Form

Source: Prepared by the researcher based on the results of the program Amos vr.24

It is evident from Table (4) that the model used by the current study is an appropriate model based on the values of the criteria. And this result leads us to the conclusion that the possibility of adopting this model because the standards have achieved their supposed limits. From it it is clear that the paragraphs of the dimensions of the customer orientation axis have participated in the interpretation of the axis in different proportions based on their estimated values.

Third: descriptive statistics

1- Continuous improvement variable

The continuous improvement variable consists of four variables

Table (5)

Results of descriptive statistics for the continuous improvement variable

dimension	Arithmetic mean	standard deviation	Relative importance	order of importance
Act	4.3177	0.48407	86	4
check	4.2255	0.58400	85	3
do	4.2113	0.64043	84	2
plan	4.1177	0.83873	82	1
Total	4.2180	0.6368	84.25	

Source: Prepared by the researcher based on the results of the program Amos vr.24

Table (5) shows the results of descriptive statistics for the continuous improvement variable, which corresponds to four dimensions (plan, do, check, correct), where the total arithmetic mean for this variable was (4.2180) and the standard deviation was (0.6368) in the language of relative importance (84.25). These statistical results indicate that a valid variable has attained a high degree of importance according to the answers of the research sample members, which indicates that the

division management works in case of non-conformance by correcting deviations and developing policies.

2- The quality of cyber security variable

The cybersecurity quality variable consists of seven variables

Table (6)

The results of the descriptive statistics of the cyber security variable

dimension	Arithmetic mean	standard deviation	Relative importance	order of importance
SRH	4.3759	0.52408	88	7
SYA	4.3475	0.55563	87	3
TDA	4.3267	0.50853	87	6
DAP	4.3085	0.52153	86	5
KSS	4.2936	0.49717	86	1
VU	4.2766	0.47123	86	4
CYA	4.2837	0.45991	86	2
total	4.3116	0.50544	86.5	

Source: Prepared by the researcher based on the results of the program Amos vr.24

Table No. (6) shows the results of the descriptive statistics for the security variable, which is measured in seven dimensions. The total arithmetic mean of this variable was (4.3116) and the standard deviation was (0.63680.50544), in the language of relative importance (86.5). These statistical results indicate that the system recovery variable after its penetration has attained a high degree of importance according to the answers of the research sample members, which indicates that the Qassim administration is working to restore the control system after its penetration by an electronic attack that seeks to disrupt the system's infrastructure and steal what is in it. of info.

3- Customer orientation variable

Table (7)

Descriptive statistics results, customer orientation

dimension	standard deviation	Relative importance	order of importance	Arithmetic mean
need	4.6043	0.34063	92	1
joy	4.5748	0.36248	91	2

Total	4.5895	0.35155	91.5	

Source: Prepared by the researcher based on the results of the program Amos vr.24

Table (7) shows the results of descriptive statistics for the customer orientation variable, which is measured in two dimensions (need and pleasure), where the total arithmetic mean of this variable was (4.5895) and the standard deviation was (0.35155), and the relative importance reached (91.5). These statistical results indicate that the need variable has attained a high degree of importance according to the answers of the research sample members, which indicates that the coupon management motivates the employee to believe that he has sufficient ability to meet the needs of his customers and at the level they expect**.**

Fourth: Testing the hypotheses of correlation

1- To test the correlation between continuous improvement and the quality of cybersecurity

The researcher used the statistical program SPSS vr. 24 In the process of finding values of correlations between the independent variable (continuous improvement) and the dimensions of the dependent variable (cybersecurity), the results are summarized in the following table:

Table (8)

The correlations between continuous improvement and the quality of cybersecurity and their dimensions

links						
		PL	DO	CH	AC	COIM
KSS	Pearson Correlation	.395**	.469**	.497**	.597**	.550**
	Sig. (2-tailed)	.000	.000	.000	.000	.000
	N	141	141	141	141	141
CYA	Pearson Correlation	.333**	.379**	.303**	.393**	.404**
	Sig. (2-tailed)	.000	.000	.000	.000	.000
	N	141	141	141	141	141
SYA	Pearson Correlation	.237**	.295**	.245**	.326**	.313**
	Sig. (2-tailed)	.005	.000	.003	.000	.000
	N	141	141	141	141	141
VU	Pearson Correlation	.119	.211*	.145	.265**	.203*
	Sig. (2-tailed)	.162	.012	.085	.002	.016
	N	141	141	141	141	141
DAP	Pearson Correlation	.018	.060	.158	.182*	.106

	Sig. (2-tailed)	.836	.480	.061	.031	.210
	N	141	141	141	141	141
TDA	Pearson Correlation	.168*	.277**	.303**	.323**	.296**
	Sig. (2-tailed)	.047	.001	.000	.000	.000
	N	141	141	141	141	141
SRH	Pearson Correlation	.140	.197*	.296**	.289**	.253**
	Sig. (2-tailed)	.098	.019	.000	.001	.002
	N	141	141	141	141	141
CYBE	Pearson Correlation	.257**	.345**	.358**	.435**	.389**
	Sig. (2-tailed)	.002	.000	.000	.000	.000
	N	141	141	141	141	141

****. Correlation is significant at the 0.01 level (2-tailed).**

***. Correlation is significant at the 0.05 level (2-tailed).**

Source: Prepared by the researcher based on the results of the program Amos vr.24

The results in Table (8) indicate that the value of the correlation between the two variables of continuous improvement and cybersecurity amounted to (0.389), which is a positive direct value with a significant level of (5%), and therefore the null hypothesis is rejected and the alternative hypothesis accepted, and we conclude that there is a significant positive correlation between continuous improvement and cybersecurity , which indicates that the management of the cybersecurity department's interest in continuous improvement will lead to an increase in the quality of cybersecurity.

1- To test the link between continuous improvement and customer orientation

The researcher used the statistical program SPSS vr. 24 In the process of finding the values of the correlations between the research variables, continuous improvement and customer orientation, and the results are summarized in the following table:

Table (9)

The links between continuous improvement and customer orientation and their dimensions

links						
		PL	DO	CH	AC	COIM
EN	Pearson Correlation	.173*	.255**	.344**	.382**	.316**

	Sig. (2-tailed)	.040	.002	.000	.000	.000
	N	141	141	141	141	141
NE	Pearson Correlation	.200*	.240**	.272**	.350**	.295**
	Sig. (2-tailed)	.017	.004	.001	.000	.000
	N	141	141	141	141	141
ORCU	Pearson Correlation	.214*	.283**	.354**	.421**	0.350**
	Sig. (2-tailed)	.011	.001	.000	.000	.000
	N	141	141	141	141	141
**. Correlation is significant at the 0.01 level (2-tailed).						
*. Correlation is significant at the 0.05 level (2-tailed).						

Source: Prepared by the researcher based on the results of the program Amos vr.24

The results in Table (9) indicate that the value of the correlation between the two variables of continuous improvement and cybersecurity amounted to (0.350), which is a positive direct value at a significant level (5%), and therefore the null hypothesis is rejected and the alternative hypothesis accepted, and we conclude that there is a direct significant correlation between continuous improvement and orientation towards the customer

2- Testing the correlation between the quality of cybersecurity and customer orientation

The researcher used the statistical program SPSS vr. 24 In the process of finding values of correlations between the two variables of cybersecurity research and customer orientation, the results are summarized in the following table:

Table (10)

Correlations between the quality of cybersecurity and customer orientation and their dimensions

links									
CYBE	SRH	TDA	DAP	VU	SYA	CYA	kss		
.345**	.220**	.399**	.301**	.218**	.194*	.170*	.371**	Pearson Correlation	EN
.000	.009	.000	.000	.009	.021	.044	.000	Sig. (2-tailed)	
141	141	141	141	141	141	141	141	N	
.271**	.204*	.245**	.156	.166*	.235**	.180*	.283**	Pearson Correlation	NE
.001	.015	.003	.065	.049	.005	.032	.001	Sig. (2-tailed)	
141	141	141	141	141	141	141	141	N	
0.354**	.242**	.372**	.264**	.222**	.245**	.200*	.376**	Pearson Correlation	ORCU
.000	.004	.000	.002	.008	.003	.017	.000	Sig. (2-tailed)	
141	141	141	141	141	141	141	141	N	

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Source: Prepared by the researcher based on the results of the program Amos vr.24

The results in Table (10) indicate that the value of the correlation between the two variables of continuous improvement and cybersecurity amounted to (0.354), which is a positive direct value at a significant level (5%), and therefore the null hypothesis is rejected and the alternative hypothesis accepted, and we conclude that there is a direct significant correlation between cybersecurity and the trend towards the customer.

Conclusions and Recommendations

A- Conclusions

1. Through the statistical results and hypothesis testing, conclusions can be drawn that will achieve the answer to the study problem and its questions and achieve its main objective. The conclusions were as follows:
2. The results showed that there is a statistically significant correlation between (continuous improvement, quality of cybersecurity, customer orientation), which contributed to improving the quality of cybersecurity, which requires the department's management to be interested in introducing continuous improvement programs and developing its employees in a way that improves the quality of cybersecurity. The quality of cyber security.
3. The department's interest in improving and developing the capabilities of its employees through training and development courses, which contributed to the department's improvement of the quality of cybersecurity with high efficiency and effectiveness.
4. The department's management is keen on stating its vision and mission for employees and applying continuous improvement through its various operations and activities, which contributes to improving the department's management ability to provide the appropriate software and hardware in order to meet the work requirements.
5. Continuous improvement processes are an essential factor in modern and successful organizations. They are a key factor for excellence and ability and an important resource to create a competitive advantage for organizations. Thus, continuous improvement processes have an important role in the National Security Agency / Cyber Security Department.
6. The results showed a significant impact of continuous improvement processes and customer orientation in the quality of cybersecurity, which contributed to improving the department's ability to organize its own work sites and improve its security operations, which requires it to develop its capabilities in the development of advanced technology capable of meeting these requirements with quality and the right time.
7. The results showed the department management's keenness to develop advanced programs that contribute to improving the ability of the studied sample to effectively provide cyber security.
8. The department's management's interest in improving mutual trust between employees and management in order to ensure the implementation of training programs and improve the effective performance of implementing customer orientation and improving the department's information base.
9. The department's management seeks to build a safe and sound database in order to ensure the flow of information to all its administrative departments, which contributes to improving the department's performance and diagnosing and analyzing threats.
10. The results showed that all variables dimensions of continuous improvement processes (plan, do, check, correct) have a positive impact on the quality of cybersecurity.
11. The department's management evaluates the performance of employees periodically, which motivates the employees themselves to continuously improve their skills and experience with the tools and equipment they use in the face of cyber threats.

b- Recommendations

In light of the findings of the study, the following recommendations can be made:

1. The department's management should be keen on motivating employees to develop their capabilities, which requires them to provide appropriate programs, tools and mechanisms in order to improve their skills in the field of cybersecurity.

2. The department's management should seek to apply continuous improvement in order to ensure the achievement of quality that gives strength and the ability to confront cyber threats.
3. The department's management should provide various programs, information and knowledge to develop employees, which requires them to develop new means and methods that encourage employees to be creative at work.
4. The department's management should encourage employees to develop their security and technical capabilities, which requires them to provide a special database.
5. The department's management should provide advanced equipment and hardware, which requires it to seize the largest possible number of opportunities available to it in order to ensure the creation of a new work pattern within the department's management.
6. The department's management should be keen on constantly updating its database in order to ensure the achievement of knowledge exchange and experiences within the department's headquarters, which requires it to transform individual knowledge in cybersecurity disciplines into collective knowledge the of it.
7. The department's management must attract highly skilled and experienced workers to work for it, which requires a high promotional process in order to attract the largest possible number of highly skilled workers, and this in turn contributes to achieving high quality in the field of cybersecurity.
8. The department's management should be keen to provide training programs that are compatible with the technology it uses, which requires it to provide an efficient and accurate database.
9. The need to improve the department's management of the internal communication capabilities between its internal departments and sections, which requires them to improve direct interaction with employees and customers.
10. The need for the department's management to develop the skills of continuous improvement among the employees in order to solve the problems and participate in making decisions that will improve the department's management's ability to prevent the shortcomings it suffers from.
11. It is necessary to invest well the continuous improvement processes in the management of the department because the knowledge of cyber security is usually not sufficiently invested. Unless continuous improvement is done properly, organizations can benefit from reducing recurring errors and creating new opportunities.
12. Emphasizing the need to provide more financial and administrative support for the ability to employ more customer orientation and continuous improvement processes in the National Security Agency / Cyber Security Department.
13. Training the department's management staff on continuous improvement to eliminate waste and thus reduce costs.
14. The department's management needs to increase the degree of use of both continuous improvement processes and customer orientation in order to increase the quality level of cybersecurity and thus increase the efficiency of the department's management

. References

1. Aburayya, A., Marzouqi, A., Alawadhi, D., Abdouli, F., & Taryam, M. (2020). An empirical investigation of the effect of employees' customer orientation on customer loyalty through the mediating role of customer satisfaction and service quality. Management Science Letters, 10(10), 2147-2158
2. Aburayya, A., Marzouqi, A., Alawadhi, D., Abdouli, F., & Taryam, M. (2020). An empirical investigation of the effect of employees' customer orientation on customer loyalty through the mediating role of customer satisfaction and service quality. Management Science Letters, 10(10), 2147-2158
3. Boyer, W. F., & McQueen, M. A. (2008). Primer Control System r Security Framework and Technical Metrics (No. INL/EXT-08-14324). Idaho National Laboratory (INL).
4. Bothur, D., Zheng, G., & Valli, C. (2017). A critical analysis of security vulnerabilities and countermeasures in a smart ship system.
5. Boyer, W. F., & McQueen, M. A. (2008). Primer Control System r Security Framework and Technical Metrics (No. INL/EXT-08-14324). Idaho National Laboratory (INL).
6. Brodin, A. (2019). A review of Sweden's السيبراني الامنr security actors through the lens of Assemblage theory.
7. Chakraborty, A. (2016). Importance of PDCA cycle for SMEs. SSRG International Journal of Mechanical Engineering, 3(5), 30-34.

8. Charantimath, P. M. (2017). *Entrepreneurship development and small business enterprise*. Pearson Education India.
9. Domi, S., Capelleras, J. L., & Musabelliu, B. (2020). Customer orientation and SME performance in Albania: A case study of the mediating role of innovativeness and innovation behavior. *Journal of Vacation Marketing*, *26*(1), 130-146.
10. Duffy, S., Bruce, K., Moroko, L., & Groeger, L. (2020). Customer orientation: Its surprising origins, tumultuous development and place in the future of marketing thought and practice. Australasian Marketing Journal (AMJ), 28(4), 181-188.
11. Düveroğlu, E. (2020). A comparative analysis of critical infrastructure cyber security policies: best practices from the US, EU and Turkey (Doctoral dissertation, Bilkent University).
12. Hawamleh, A. M. A., Alorfi, A. S. M., Al-Gasawneh, J. A., & Al-Rawashdeh, G. (2020). cyber Security and Ethical Hacking: The Importance of Protecting User Data. *Solid State Technology*, *63*(5), 7894-7899.
13. He, H., Wang, W., Zhu, W., & Harris, L. (2015). Service workers' job performance: The roles of personality traits, organizational identification, and customer orientation. European Journal of Marketing
14. KANG, M. J., WU, Z., & HWANG, H. J. (2021). A Study on the Mediating Effect of Customer Orientation between O2O Service Quality and Customers' Perceived Service Satisfaction. Journal of Distribution Science, 19(2), 37-44.
15. Lamba, A., Singh, S., Balvinder, S., & Rela, S. (2015). To Classify cyber-Security Threats in Automotive Doming Using Different Assessment Methodologies. International Journal For Technological Research In Engineering, 3(3).
16. Lee, C. M. J., Che-Ha, N., & Alwi, S. F. S. (2021). Service customer orientation and social sustainability: The case of small medium enterprises. Journal of Business Research, 122, 751-760.
17. Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2019). cyber security management model for critical infrastructure.
18. Lizarelli, F. L., de Toledo, J. C., & Alliprandini, D. H. (2021). Relationship between continuous improvement and innovation performance: an empirical study in Brazilian manufacturing companies. *Total Quality Management & Business Excellence*, *32*(9-10), 981-1004.
19. Marouni, H. (2017). The ISO 9001: 2015 Implementation Handbook: Using the Process Approach to Build a Quality Management System. Quality Progress, 50(5), 61-61
20. Meiling, J., Backlund, F., & Johnsson, H. (2012). Managing for continuous improvement in off-site construction: Evaluation of lean management principles. Engineering, Construction and Architectural Management.
21. Mishra, N. (2020). The Trade:(cyber) Security Dilemma and Its Impact on Global cybersecurity Governance. Journal of World Trade, 54(4).
22. Muzumdar, P., & Kurian, G. (2021). Empirical study to explore the influence of salesperson's customer orientation on customer loyalty. arXiv preprint arXiv:2103.01220.
23. Pipyros, K., Thraskias, C., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2018). A new strategy for improving r-attacks evaluation in the context of Tallinn Manual. Computers & Security, 74, 371-383.
24. Ritamaki, A. (2017). Applying Continuous Improvement in Order to Reach Operational Excellence.
25. Sanchez, L., & Blanco, B. (2014). Three decades of continuous improvement. *Total Quality Management & Business Excellence*, *25*(9-10), 986-1001. https://doi.org/10.1080/14783363.2013.856547.
26. Shyng, J. H. (2021). The Practice of Deming Cycle Improvement Mechanism in Climate Change Environmental Education. Journal of Contemporary Educational Research, 5(8), 205-214.
27. Silva, A. S., Medeiros, C. F., & Vieira, R. K. (2017). Cleaner Production and PDCA cycle: Practical application for reducing the Cans Loss Index in a beverage company. Journal of cleaner production, 150, 324-338.
28. Singh, S., & Silakari, S. (2009). A survey of cyber attack detection systems. International Journal of Computer Science and Network Security, 9(5), 1-10.
29. Soita, J. J. (2016). Continuous improvement practices and product quality performance at TATA chemicals Magadi limited (Doctoral dissertation, University of Nairobi).
30. Teoh, C. S., & Mahmood, A. K. (2017, July). National الامن السيبراني r security strategies for digital economy. In *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 1-6). IEEE.
31. Veale, M., & Brown, I. (2020). cybersecurity. Internet Policy Review, 9(4), 1-22.
32. Vélez Arias, S. A. (2020). Effective Work Order Requests And Scheduling Tool Design for Maintenance Jobs. Manufacturing Engineering;.
33. Vlad, D. E. (2019). Concepts of quality connected to social media and emotions. Springer Nature.