PalArch's Journal of Archaeology of Egypt / Egyptology

RELATIONSHIP BETWEEN CONTINUOUS IMPROVEMENT AND QUALITY CYBERSECURITY

Aseel Ali Mezher[1], Amir Sajit Mdlool [2]

[1,2] University of A1-Qadisiyah / College of Administration and Economics/ Business Administration Department.

Email: [1]aseel.mezher@qu.edu.iq [2]admin.mang21.11@qu.edu.iq

Aseel Ali Mezher, Amir Sajit Mdlool, Relationship Between Continuous Improvement and Quality Cybersecurity, Palarch's Journal of Archaeology of Egypt/Egyptology 19(2), 365-377. ISSN 1567-214x.

Keywords: Continuous Improvement, Quality Cybersecurity.

ABSTRACT:
Current research aims to highlight the impact of continuous improvement in cybersecurity quality. The research adopted the identification as a basic measurement tool for collecting data from the sample in question, which amounted to 141 of the 150 affiliates of the cybersecurity department of the Iraqi National Security Service, where it was employed to test the main and subsidiary research hypotheses through the use of a number of statistical means, most notably (SPSS vr. 20, AMOS vr. 20) The results of the research have proved the most valid hypotheses, and the research has reached a set of conclusions, most notably that there is a role for continuous improvements in the work of the National Security Service/Cyber Security Department.

INTRODUCTION:

Continuous improvement is one of the important management concepts and one of the most important features of activities affecting the quality of work, and being an important factor in the success of all organizations has increased organizations' interest in them in the past few years. The large digital transformation and the predominant trend of organizations to digitize to achieve their goals have made it imperative for them to keep pace with continuous improvements. The use of new technologies may improve efficiency and security but also increase cyber risks. As

cybersecurity is not just a technical issue, it is also a strategic and political issue that touches everyone and everyone bears responsibility for it.

PART ONE: RESEARCH METHODOLOGY

Search Problem

The problem of research is the nature of the role those continuous improvements in the quality of cybersecurity and the nature and size of the relationship and its impact. Accordingly, the problem of research can be asked with the following qualitative questions:

a. How well are cybersecurity staff aware of the importance of continuous improvement processes?
b. What is the level of cybersecurity in the research section and is the section's staff aware of the sensitivity and importance of this subject?
c. Is there an impact of continuous improvements in cybersecurity quality?

Research Importance

The importance of research is to measure the nature and type of relationship between continuous improvement and cybersecurity, through the following:

Scientific Importance

The scientific significance of this research stems from the fact that research topics (continuous improvement, cybersecurity) are important topics that have received the attention of a large number of researchers.

Practical Importance

The practical importance of this research is highlighted by the contribution of its results in assisting the sample researched in formulating a good strategy that contributes to demonstrating the importance of improving cybersecurity in the sample researched, as well as drawing the attention of the sample researched to the use of continuous improvement mechanisms that would raise the level of cybersecurity to quality.

Research Objectives

a. Identify the level of continuous improvement in the search sample cybersecurity department.
b. Recognize the reality of the quality of security services provided in the research section.

c. Provide a comprehensive picture of current cybersecurity trends by identifying which areas need improvement in the cybersecurity requirements of the research department.

Data And Information Collection Tools

For the purpose of completing the requirements of the theoretical aspect of the research, the researcher relied on Arab and foreign references from books, studies, letters, scientific dissertations, publications, periodicals and research related to the research, as well as the use of the International Information Network (Internet). The researcher relied on field research to collect sample data by adopting the questionnaire as the main means of collecting data and information, and being the most consistent with current research.

Research Hypotheses

In order to supplement the requirements of the search and to answer its questions, the following hypotheses have been made:

a. There is a statistically significant correlation between continuous improvement and the quality of cybersecurity.
b. There is a direct statistically significant effect between continuous improvement and the quality of cybersecurity.

Research Community and Sample

The target community for the study consists of all the 150 affiliates in the cybersecurity department of the Iraqi National Security Service (NSS). The number of questionnaire forms distributed to the search sample is 150, 141 of which have been approved only for their validity to analyze and leave the rest either for non-return or lack thereof.

Research Outline

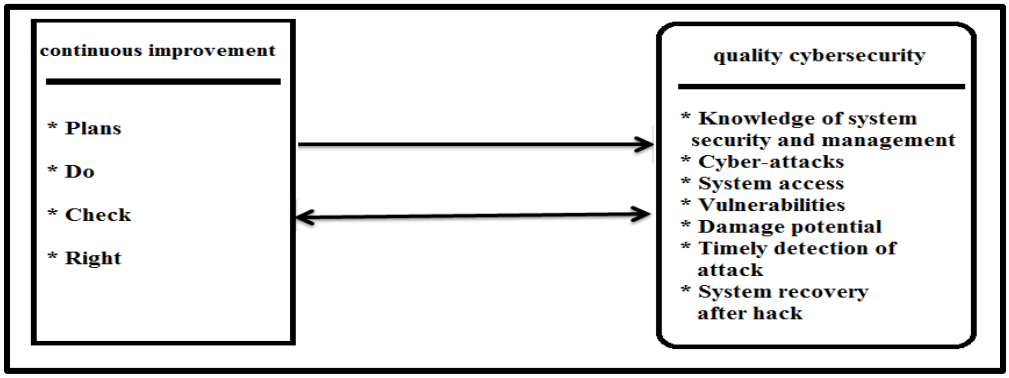

Figure (1) Hypothetical Diagram for Research

PART TWO: THEORETICAL ASPECT

First. Continuous Improvement

Concept Of Continuous Improvement

Continuous improvement is defined as an increased and sustained effort to improve products, processes and services. Continuous improvement should be seen as a process aimed at achieving improvement "rather than a series of isolated improvement activities. Continuous improvement is described as a process within the most comprehensive quality improvement strategies (Meiling et al., 2012:141). considers that (Singh & Singh,2015:3) there is a continuing need to maintain a low cost of quality, reduce damage, reduce production lines, and accelerate manufacturing to achieve and maintain competitiveness. Much of this can be done by implementing continuous improvement. argues that (Kenyon & Sen, 2016:120) organizations must continuously improve their operations in manufacturing and service delivery environments in order to maintain their competitiveness. These improvements include reducing variability and increasing efficiency and effectiveness. These types of improvements often increase capacity, productivity, flexibility and responsiveness, and thus lead to greater profitability.

Dimensions Of Continuous Improvement

We represent the dimensions of continuous improvement obtained by consensus from most writers and researchers as follows:

a) **Plans**: The first PDCA course procedure is planning in this procedure, senior management should examine ongoing activities and develop a plan in case of any problems, requiring data collection, identification, screening and use to build an effective plan and accurate performance appraisal procedures (Luthra et al., 2020:117).
b) **Do**: This phase is where the developed plan is implemented in order to make changes in the process in the organizations (in order to raise their productivity or quality and remove the causes of problems) and this is done with the support and understanding of management. At this stage, tools such as work schemes, performance measurement, flow charts or checklists can be used (Kocik, 2017:2).
c) **Check**: From (Coleman,2015:17) point of view, this stage is as follows:

1. Compare actual versus expected results
2. Document lessons learned, knowledge gained and any sudden results that have emerged.
3. Conduct a root cause analysis if necessary

d) **Right**: This phase represents the culmination of planning, testing and analysis. Action is taken based on what has been learned in the inspection step (Hakim et al., 2020:876).

Importance Of Continuous Improvement:

The importance of continuous improvement in the business environment stems from three main phenomena: - changes in the business environment and the emergence of new management systems and the importance of quality management itself, and organizations must focus on eliminating waste and identifying new areas of improvement. (Sanchez&Blanco,2014:2). Abbas, 2017:166) believes that it is essential for all CQM systems to improve the quality of the products and services provided by the organizations. This quality improvement results in greater productivity and enhances the organizations' ability to remain vital and work to recruit people and provide services, focus on continuous quality and help organizations to do things right.

Objectives Of Continuous Improvement

sets (Shareaa et al., 2020:557) objectives for continuous improvement as follows:

a) Increased levels of organizations' satisfaction
b) Achieve efficiency and high quality in performance.
c) Reduce losses.
d) Cost reduction.
e) Increase productivity.

Second: Cybersecurity Quality

Concept Of Quality

Quality as a philosophy is to strive for perfection by embracing sustainable continuity, while some refer to quality in terms of its different standards and this definition is limited at best (Davis, 2017:75). (Vlad,2019:17) confirms that there are two main points of view in determining quality: -

a) Quality is conforming to specifications - this view reflects the view of the manufacturer organization.
b) Quality is compatibility with customer needs - this ray reflects the customer's view.

Cybersecurity

Concept of Cybersecurity

It is believed (Düveroğlu, 2020:44) that the concept of cybersecurity refers mainly to the protection of computer systems from theft or damage to their devices, software or databases, and even to the disruption of operations and services they provide to the community. states that(Tvaronavičienė et al., 2020:803) the introduction of cybersecurity has led to a significant development in the role and responsibility of the State towards its citizens. Given that cyberattacks are a growing phenomenon, especially in developed countries, many of them have decided to implement newer strategies, taking into account cybersecurity in the private and public spheres. According to the International Telecommunication Union (ITU), by the end of 2018, 3.9 billion people were using the Internet. (Plachkinova et al., 2021:6203) indicates that cybersecurity affects all aspects of regulatory management, with regulatory systems, networks and infrastructure increasingly being targeted by malicious actors identified with advanced skills and resources. Such attacks have the potential to cause significant disruption to our society, including damage to assets, people and the environment. (While Alexi, 2021:86), believes that under new global conditions, there is an increasing need to ensure information security, in the context of the dramatic shift of data for different organizations to virtual space. Cybersecurity (Düveroğlu,2020:440 is defined as protecting computer systems from theft or damage to their devices, software or databases, and even from disruption of operations and services they provide to the community. While (Creese et al., 2021:1) defined it as techniques, processes and policies that help prevent and/or reduce the negative impact of events in cyberspace that can occur as a result of deliberate actions against IT by a hostile or malicious actor.

Dimensions Of Cybersecurity

1. **Knowledge of system security and management:** is the full knowledge of the security and management of the system and the ideal condition it must be, including the structure according to which network links and contracts, called Network Topology, which may be a physical topology (physical) or a logical topology, as well as routes of communication and normal operational behaviour of the system and everything related to it (Boyer & Queen,2008:2).
2. **Cyber-attacks:** Use a deliberate procedure to alter, disable, deceive, weaken or destroy hostile computer systems, networks, information and/or software in such systems or networks or passing through such systems or networks (Pipyros et al., 2018:5).
3. **System access:** Accessibility is a legal mandate, and the need for accessibility assumes importance worldwide. In 2018, in the United States

of America alone, there were 2,285 web access lawsuits.. (Renaud,2021:12).

4. **Vulnerabilities:** It is the degree to which an attacker can affect the system (Tupper et al., 2008:3).

5. **Damage potential**: Potential to exploit vulnerabilities and damage. (Lamba et al., 2015:5834)

6. Timely detection of attack: In recent years, the number of attacks on networks has increased significantly, with interest in detecting cyberattacks among researchers increasing (Singh & Silakari, 2009:1).

7. **System recovery after hack**: The ability to restore the control system from a hacked state to a relentless state. Includes the reliability of backup and recovery facilities and the time needed to recover from an attack (Boyer & Queen,2008:2).

Importance Of Cybersecurity:

Cybersecurity (Goutam, 2015:14) is an important part of individuals and families, as well as organizations, governments, educational organizations and daily businesses, and it is essential for families and parents to protect children and family members from online fraud. believes (Salminen,2015:1) that in order to protect society's vital functions in all security situations, the Government has initiated the cybersecurity strategy and implementation process. argues that (Vozikis et al., 2020:1) the importance of cybersecurity is to protect critical infrastructure that has become an ideal target for government and criminal groups due to its large offensive surface of interlocking IT and operations technology networks.

Objectives of Cybersecurity

believes (Yampolskiy & Spellchecker,2016:1) the main objective of cybersecurity is to reduce the number of successful attacks on the system. see that (Al-Khadra and others, 223:2020) there are several goals behind the application of cybersecurity. These objectives are as follows:

1 Secure private information and data security infrastructure.

2 Protecting the information and communications network from any potential penetration, which plays a key role in the flow of information and data from the service provider to the future.

3 Encrypt digital transactions so that no hacker can attack them or tamper with their content.

PART THREE: PRACTICAL ASPECT

First: Coding and Characterization

Data analysis with ease and credibility, accurate results that require a set of symbols that facilitate statistical analysis of the data in the analysis, and table (1) shows the description and symbolization of the variables and dimensions of the research.

Table (1) Coding and Characterization of Search Variables

variables		**No.**	**Cod**
continuous improvement	Plans	5	PL
	Do	5	DO
	Check	5	CH
	Right	5	AC
quality cybersecurity	Knowledge of system security and management	5	KSS
	Cyber-attacks	5	CYA
	System access	4	SYA
	Vulnerabilities	4	VUI
	Damage potential	4	DAP
	Timely detection of attack	3	TDA
	System recovery after hack	4	SRH

Second: General statistics

Some general statistics have been identified to reveal their characteristics such as computational medium calculation, standard deviation and difference factor.

Variable Continuous Improvement

Continuous improvement variable consists of four variables

Table (2) Results of the descriptive statistics of the continuous improvement variable

dimension	mean	S.D	%	order of importance
AC	4.3177	0.48407	86	4
CH	4.2255	0.58400	85	3
DO	4.2113	0.64043	84	2
PL	4.1177	0.83873	82	1
Total	4.2180	0.6368	84.25	

Table 2 shows the results of the statistical description of the continuous improvement variable, measured in four dimensions, where the total arithmetic average of this variable (4.2180), standard deviation (0.6368) and relative importance language (84.25). These statistical findings indicate that a valid variable has gained a high degree of relevance according to the responses of the research sample individuals indicating that, in the event of mismatch, partition management works by correcting deviations and developing policies.

Cybersecurity Variable

Table (3) Results of the Serrani Security Variable Descriptive Statistics

dimension	mean	S.D	%	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	

Table 3 shows the results of the statistical description of the Cyber Security Variable measured in seven dimensions, where the total calculation average of this variable (4.3116) and standard deviation (0.63680.50544) in relative importance language (86.5). These statistical findings indicate that the system restoration variable after its penetration has gained a high degree of relevance according to the responses of the search sample personnel indicating that the partition management is working to restore the control system after its penetration by an electronic attack that seeks to disrupt the system's infrastructure and steal its information.

THIRD: TEST HYPOTHESES

Test Correlation Between Continuous Improvement and Cybersecurity

The researcher has used the statistical program SPSS vr. 20 In the process of finding correlation values between the independent variable (continuous improvement) and the dimension of the subordinate variable (cybersecurity) and the results are summarized in the following table:

Table (4) correlations between two variables and their dimensions

continuous improvement	Right	Check	Do	Plans	
.550**	.597**	.497**	.469**	.395**	**Knowledge of system security**
.404**	.393**	.303**	.379**	.333**	**Cyber-attacks**
.313**	.326**	.245**	.295**	.237**	**System access**
.203*	.265**	.145	.211*	.119**	**Vulnerabilities**
.106**	.182*	.158	.060	.018**	**Damage potential**
.296**	.323**	.303**	.277**	.168*	**Timely detection**
.253**	.289**	.296**	.197*	.140**	**System recovery**
.389**	.435**	.358**	.345**	.257**	**quality**

the previous table indicate that the correlation value between continuous improvement variables and cybersecurity was 0.389, a morale-level expulsion value (5%). Thus, the zero hypothesis is rejected and the alternative hypothesis is accepted and we conclude that there is a moral pecuniary correlation between continuous improvement and cybersecurity, which shows that the interest of cybersecurity management in continuous improvement will increase the quality of cybersecurity.

Impact Test between Continuous Enhancement and Cyber Security

1. The results indicate that there is a direct moral and expulsive effect at a moral level (5%) of the continuous improvement variable in cybersecurity as the impact value (0.389) reached a critical value of (6.946).

Table (5) Criteria for Structural Modeling Equation SEM

path			estimate	S.E.	C.R.	P
continuous improvement	--->	**quality cybersecurity**	0.389	0.056	6.946	***

PART FOUR: CONCLUSIONS AND RECOMMENDATIONS

Conclusions

1. The results showed a significant correlation between (continuous improvement, and quality of cybersecurity) which contributed to improving the quality of cybersecurity, which requires the department's management to be interested in the development of continuous improvement programs and the development of its workers in a way that improves the quality of cybersecurity.
2. The department's interest in improving and developing the potential of its employees through training and development courses contributed to improving the department's quality of cybersecurity efficiently and effectively.
3. The Department Management is keen to demonstrate its vision and mission to the employees and apply continuous improvement through its various processes and activities, which contributes to improving the Department's management ability to provide appropriate software and hardware in order to meet the business requirements.
4. Continuous improvement processes are an essential factor in modern and successful organizations. They are a key factor of excellence, ability and an important resource for creating a competitive advantage for organizations. Continuous improvements thus have an important role to play in the National Security Service/Cybersecurity Department.

Recommendations

1. The department's management should be keen to motivate workers to develop their capabilities, requiring them to provide appropriate programs, tools and mechanisms to improve their cybersecurity skills.
2. The department's management should seek to apply continuous improvement in order to ensure the quality gained by the strength and ability to counter cyber threats.
3. The department's management should provide various programs, information and knowledge to develop workers, which requires it to develop new methods and methods that encourage workers to be creative at work.
4. The department's management should encourage workers to develop their security and technical capabilities, requiring them to provide a private database.

REFERENCES

Vegetable, C., Salami, E., Clippy, N., & Grace. (2020). Cybersecurity and artificial intelligence in Saudi universities. Journal of University Performance Development, 12 (1), 217-233.

Abbas, J. (2020). The impact of total quality management on an organization's sustainability through the intermediate impact of knowledge management. Journal of Sleaner Production, 244, 118806.

ALEXEI ،A. (2021). Ensuring information security in public organizations in the Republic of Moldova through standard. International Organization for Standardization 27001

Al-Shareaa, I. H. D., Al-Azzawib, R. Z. A., & KHhudhairc, A. H. (2020). Tax culture and its impact on tax activity (applied research on the public tax authority). International Journal of Innovation, Creativity and Change, 10 (11), 531-551

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).

Creese, S., Dutton, W. H., & Esteve-González, P. (2021). Social and Cultural Formation Cybersecurity Capacity Building: A Comparative Study of Countries and Regions. Personal and Ubiquitous Computing, 1-15.

Duviroglo, e. (2020). Comparative Analysis of Critical Infrastructure Security Cybersecurity Policies: Best Practices from the United States, the European Union and Turkey (Doctoral Thesis, University of Belkent).

Goutam, R. K. (2015). Importance of Cyber Security International Journal of Computer Applications, 111 (7).

Hakim, L., Rosadi, K. I., El Widdah, M., Us, K. A., Shalahudin, S., & MY, M. (2020). Has the PDCA course, service quality and innovation ability affected the performance of private universities? Methodological reviews in pharmacy, 11 (10), 874-833.

Jagusiak-Kocik, M. (2017). PDCA course as part of continuous improvement in the case study of the production company. Production Engineering Archives, 14. https://scholar.googleusercontent.com/scholar.

Kenyon, G. N., & Sen, K. C. (2016). Perception of quality. Springer London Limited. https://link.springer.com/book/10.1007%2F978-1-4471-6627-6.

Lamba, A., Singh, S., Balvinder, S., & Rela, S. (2015). Classification of cybersecurity threats in car dome using different assessment methodologies. International Journal For Technological Research In Engineering, 3 (3) .

Luthra ،S. ،Garg ،D. ،Agarwal ،A. ،& Mangla ،S. K. (2020). Total Quality Management (TQM): Principles, Methods and Applications. Convention on the Rights of the Child Press.

Meiling, J., Backlund, F., & Johnsson, H. (2012). Management for continuous improvement in off-site construction: assessment of poor management principles. Engineering, Construction and Architectural Management

Pipyros ،K. ،Thraskias ،C. ،Mitrou ،L. ،Gritzalis ،D. ،& Apostolopoulos ، T. (2018). A new strategy to improve the assessment of attacks in the context of the Tallinn Manual. Computers and Security, 74, 371-383.

Plachkinova, M., Steiner, S., Conte De Leon, D., & Shepherd, M. (2021). Introduction to Minitrack on Organizational: Advanced Defense, Analytics and Security.

Renaud, K. (2021, February). Cybersecurity is accessible: the following limits? In ICISSP (page 9-18).

Salminen, M. (2015). Cybersecurity Government Security as National Security.

Sanchez, L., & Blanco, B. (2014). Three decades of continuous improvement. Total Quality Management and Business Excellence, 25 (9-10), 986-1001. https://doi.org/10.1080/14783363.2013.856547.

Singh, J., & Singh, H. (2015). Review and guidance the continuous improvement of philosophy and literature. Benchmarks: Journal. International

Singh, S., & Silakari, S. (2009). Survey of cybersecurity attack detection systems. International Journal of Computer Science and Network Security, 9 (5), 1-10.

Tupper, M., & Zincir-Heywood, A. N. (2008, March). VEA-bility Security Scale: Network Security Analysis Tool. 2008 Third International Conference on Availability, Reliability and Security (p. 950-957). IEEE.

Security management of critical energy infrastructure in national strategies: cases of the United States of America, the United Kingdom, France, Estonia and Lithuania. Insight into regional development, 2 (4), 802-813.

VLAD, DE (2019). Quality concepts associated with social media and emotions. Springer Nature.

Vozikis ،D. ،Darra ،E. ،Kuusk ،T. ،Kavallieros ،D. ،Reintam ،A. ،& Bellekens ،X. (2020). On the importance of cybersecurity training for operators of multi-vector power distribution systems. In Proceedings of the 15 International Conference on Affaire, Reliability and Security (pp. 1-6) .

Yampolskiy, R. V., & Spellchecker, M. S. (2016). AI Safety Cybersecurity: A timeline for AI failure. arXiv preprint arXiv:1610.07997.