Salud, Ciencia y Tecnología - Serie de Conferencias. 2024; 3:670
doi: 10.56294/sctconf2024670

Category: Finance, Business, Management, Economics and Accounting

ORIGINAL

Managing Cyber Security Costs for Sustainable Competitive Advantage

Gestión de los costes de ciberseguridad para una ventaja competitiva sostenible

Sahar Yass AL-Asady[1], Inaam Mohsin Almusawi[2], Karrar Abdulellah Azeez[2]

[1]Directorate of Najaf Education, Najaf, Iraq.
[2]University of Kufa, Collage of Administration and Economics, Najaf, Iraq.

Cite as: AL-Asady SY, Almusawi IM, Abdulellah Azeez K. Managing Cyber Security Costs for Sustainable Competitive Advantage. Salud, Ciencia y Tecnología - Serie de Conferencias. 2024; 3:670. https://doi.org/10.56294/sctconf2024670

Submitted: 05-01-2024 **Revised:** 02-04-2024 **Accepted:** 30-06-2024 **Published:** 01-07-2024

Editor: Dr. William Castillo-González

ABSTRACT

Because of information technology, accounting systems need to manage cyber security operations. Cyber security plays a critical role and controlling information has become challenging task. The firms should measure and the costs related with applying cyber security plans. We developed a thinking to know the cyber security costs and the dimensions within the cyber security Framework produced by the airport affect on sustainable competitive advantage in response to the cyber security Improvement. The population consists of 6 airports in Iraq, and the sample size was 232 employers. The hypotheses formulated were tested with F-test statistics using Eviews software package version 12. This study focuses on the cyber security costs in the international era may be easily adopted by firms that are interested in improving competitive advantage. Findings show that managing and constantly improving cyber security operations costs positively have affected sustainable competitive advantage. The paper argued that changes in the sustainable competitive advantage that should be segmented in cost accounting systems to reflect whether those tasks are being performed as fit. Then, the conclusion for companies may also wish to customize the plans to better performance with their unique systems, structures, and work processes.

Keywords: Cyber Security; Costs Managing; Accounting Profession; Cyber Attacks; Competitive Advantage.

RESUMEN

Debido a la tecnología de la información, los sistemas contables necesitan gestionar operaciones de ciberseguridad. La ciberseguridad desempeña un papel fundamental y el control de la información se ha convertido en una tarea difícil. Las empresas deben medir y los costes relacionados con la aplicación de planes de ciberseguridad. Desarrollamos una reflexión para conocer los costes de ciberseguridad y las dimensiones dentro del Marco de ciberseguridad producido por el aeropuerto afectan a la ventaja competitiva sostenible en respuesta a la Mejora de la ciberseguridad. La población está formada por 6 aeropuertos de Irak, y el tamaño de la muestra fue de 232 empresarios. Las hipótesis formuladas se comprobaron con la estadística F-test utilizando el paquete de software Eviews versión 12. Este estudio se centra en los costes de la ciberseguridad en la era internacional puede ser fácilmente adoptado por las empresas que están interesadas en mejorar la ventaja competitiva. Los resultados muestran que la gestión y la mejora constante de los costes de las operaciones de ciberseguridad han afectado positivamente a la ventaja competitiva sostenible. El documento argumentó que los cambios en la ventaja competitiva sostenible que deben ser segmentados en los sistemas de contabilidad de costes para reflejar si esas tareas se están realizando en forma. A continuación, la conclusión para las empresas también puede desear personalizar los planes para un mejor rendimiento con sus sistemas únicos, estructuras y procesos de trabajo.

Palabras clave: Ciberseguridad; Gestión de Costes; Profesión Contable; Ciberataques; Ventaja Competitiva.

INTRODUCTION

The world's interest in airport services is increasing because of its impact on our daily lives, and the focus comes on the quality of this service due to the growing need, especially the Internet service, in the exchange of news and information between members of society and the airport management and between other countries, and we live in the information and communication revolution. Users of airport security programs are interested in Communication services with speed and quality of transfer and exchange of information. Therefore, the systems in airports in many countries of the world have undergone a major transformation thanks to digital technology, as it has contributed to lowering costs and improving the management of its operations by providing the best services to customers (Bulto, & Kant, 2023). This may undermine customers' confidence in their security systems and threaten the safety and confidentiality of their data. Despite the increase in cyber-attacks, airport security systems throughout Iraq are still lagging behind in terms of cyber readiness - that is, the ability to confront cyber-attacks compared to other sectors or service units. In the countries of the world, it should be noted here that planning for cyber security involves spreading awareness of the importance of globalization; it lacks the investments and support required for it, as it faced a stumbling block represented in the use of outdated airport management information systems (Muravskyi, 2021). These investments can be directed to creating an initial cyber security system that will be the cornerstone of a larger and broader system. Airport systems often contain financial details and numbers as well as confidential and sensitive information, which make airports a particularly attractive target for cybercriminals. Airports also often rely on secured systems. Airports are badly damaged and vital to their operations, so the airport sector has been a ripe target for cybercrime. Ransom ware attacks on airports have become commonplace, with regular attacks taking place around the world.

It seems that any damage from cybercrime to airport security will cause higher costs than those resulting from natural disasters. The problem of study is knowledge lack to present the impact of cybersecurity costs on achieving a sustainable competitive advantage in airports and the research problem can be formulated by question Does data enhancement has a role for achieving sustainable competitive advantage in airports? The paper is divided into five sections as. Section 1 shows the introduction. Section 2 presents a literature review. Section 3 describes the research methodology. Section 4 is a discussion of results. Section 5 discusses the conclusion of the study.

Literature review

The cyber security costs: The economics of cyber security protecting the confidentiality, integrity, and accessibility of information requires time, effort, and money. Research on cyber security costs dates back nearly two decades, and has mostly focused on two topics: budgeting appropriately, and quantifying the economic impacts of cyber-attacks. (Radziwill & Benton, 2017) studied the economic impacts of cyber security breaches using stock market performance. As an indicator, by creating models that estimated stock valuations in the absence of an attack, and comparing them to stock performance after the attacks, they found a detectable drop in stock prices only after attacks that involved unauthorized access to confidential data (Muravskyi,2021). Cyber security, or what is sometimes known as information technology security, can be defined as "a set of procedures that require protection of networks, computer hardware, all programs and information from any attack, theft, damage or access to the violator" and is also known as "the mechanism of individuals and institutions to reduce the risks of cyber-attacks" (Li , & Liu, 2021). (Ghelani) defines cyber security as "a set of technical, administrative and organizational means that are used in order to prevent unauthorized use, as well as prevent misuse, and restore all electronic information and communication systems and the information they contain, in order to ensure the continuity of the work of information systems and work to protect And the confidentiality and privacy of personal data, and taking technical and practical measures, to protect citizens and consumers from the potential risks of cyberspace (Ghelani, 2022) As for the definition of cyber security costs as "the hidden costs paid by economic units, institutions and consumers, for direct losses, in making more efforts to accelerate service recovery, address business disruptions, and repair damage to employee morale and customer confidence" (Von Solms & Van Niekerk, 2013).

Hejase defines cyber security costs as "the costs of non-monetary losses in productivity, lost work hours, and the cost of damages Catch up with the performance of national unity and economies" (Hejase et al.,2021). The European system defined the costs of cyber security as the ability of the information system to resist all hacking attempts that mainly target data or defensive means that would thwart attempts by hackers and the consequences costs borne by the economic unit. Cyber security is constantly evolving, and sustainable approaches will be needed by countries to ensure that all digital software and solutions remain secure, reliable

https://doi.org/10.56294/sctconf2024670

and trustworthy, and perhaps one of the lessons learned from the Corona pandemic crisis is that collective problems related to the provision of services or cyber security need to be addressed Through multiple and comprehensive technical approaches formulated by developed countries that are skilled in mastering the mechanisms and requirements of cyber security(Singh, & Singh, 2022).

Cyber security components: There are three elements on which cyber security depends mainly, which are confidentiality, validity and integrity of information, and complementarity in the availability of information, which are as follows, (John , & Thomas, (2019,(Antczak, 2020,((Muravskyi,2021. (

1- Confidentiality: the confidentiality of data or information is intended to be preserved by granting permission to only those authorized to access that information or data, and to prevent unauthorized persons from accessing that data with the necessity of not disclosing and leaking it to unauthorized persons.

2- Integration and integrity of information: It is intended to preserve such data or information from modification, change, deletion or addition, except by qualified or specialized persons.

3- Availability and Availability of Information: This refers to the availability of such data or information by specialized persons and their availability at the appropriate time.

Cyber security aims to secure the protection of financial and human resources associated with information and communication technologies. And obtaining a sufficient amount of information security so that the wheel of production does not stop, and the damage does not turn into permanent losses in the face of the risks of technology and information. (Muravskyi, 2021), (Singh, & Singh, 2022)

Types of cyber security costs: In order to appropriately manage cyber risks, there must be an informed understanding of the true costs of cyber security breaches. Qualitative analysis in previous surveys of cyber security breaches for many organizations found that units tend to overlook indirect, long-term, and intangible costs when considering the impact of a cyber security breach or attack. They do not fully account for direct losses, due to a lack of transparency. Awareness and accurate understanding of these costs, which made it an obstacle to the ability of units and institutions to make risk-based investment decisions, so it is necessary to provide a basis for understanding the real costs of cyber security breaches and attacks in order to better direct resources when managing and mitigating electronic risks, for many cyber-crimes Of the costs include: (Romanowski, 2016), (Radziwill, & Benton, 2017), (Aleksey Savkin,2021); (Furnell, et al.,2020),(Bulto, & Kant, 2023):

-1 The costs of protecting the infrastructure of the system: These costs include the costs of protecting resources, software and personnel, and include. The costs of the cyber security protection system against viruses, programs, systems, suspicious activities, and malicious software for management information systems on devices. Costs of electricity and communications cables that transmit data that support cyber security services are protected from tampering or damage. The technical governance system to provide cyber security for electronic transactions.

Alternative software costs in the event of failure or interruption in business performance. There are plans to restore business to normal within a planned time frame, and the costs of training employees and administrators on the requirements of achieving cyber security.

2- Regulatory Action Costs: These costs include: the costs of preventive insurance measures for employees in charge of electronic transactions. Costs of records and documentation for all resources of the cyber security system. Backup memory costs to record the errors that occur in the cyber security system through reports and all actions taken to correct them are mentioned.

3- External support costs: These costs are included costs of contracting with external parties in the field of developing information systems and cyber security. The costs of information systems to obtain consultations in the cyber security system.

4-The costs of information systems protection experts: those work in cyber security centers.

5- The costs of international participants: report any security gaps they notice in the systems.

6- Costs of cyber security developing and management: included enhancing the information technology infrastructure to ensure enhanced cyber security. The effectiveness of protection programs to prevent attempts to penetrate and infringe on the information system at airports. Senior management support for a successful cyber security policy adopting the use of biological means in determining the identity and authority of the users of the cyber security system. Setting controls for exchanging information with the concerned authorities outside the airport Most of these cost.

In addition, these costs are identifiable, so we must take them into account when assessing the impact of cybercrime (Zana & Eugenia: 2020). There are costs to take into account which are the costs of system downtime i.e. downtime is the corollary result of an IT security incident – the time during which technology and systems cannot be used in their normal level of functionality, whether ransom ware blocks access to enterprise systems and data or needs to be reset. Appointed to counter interference, the removal of access

https://doi.org/10.56294/sctconf2024670

to technological systems greatly affects organizations and can prevent the regular development of operations, which affects both employees and consumers together and includes (direct costs the cost of forensic analysis, fines and compensation to customers, and indirect costs refer to the loss of customers, employees and existing partners and the potential that occurred due to the data breach (Zana, & Eugenia, 2020),(Antczak, 2020).

Cybercrimes are carried out according to very modern methodologies and methods with a higher technological dimension than traditional crimes. It was very necessary for cyber security to come in order to overcome this problem in order to keep pace with technological development. The cyber security is tracking and detection to discover and trace electronic crimes, and thus overcome them. It also speeding to provide electronic crimes is represented by the use of modern technologies developed by hackers, and it is necessary for cyber security to come with modern and highly efficient technologies that exceed their techniques and expertise. (Venkatachary & Samikannu, 2017).

The Cyber security need to some requirements in terms of costs. The availability of appropriate mechanisms for the implementation of work policies so that there is clarity on how to implement such policies and to determine the penalties that will be expected in the event of a breach. And needing to pay attention to human resources through the management and operation of information networks for efficient, trained and qualified human elements to deal with technology and modern techniques (Radziwill, & Benton, 2017). Moreover, it provides a kind of monitoring and follow-up of data activities and all information available through the network in an accurate and permanent way in order to discover any suspicious and abnormal movements within the scope of the network. The importance is to operate encryption protocols through identity verification and data encryption systems, in order to secure information on the network and to choose world-famous programs in this field (Bulto, , & Kant, 2023).

The sustainable competitive advantage:

Sustainable competitive advantage can be defined as the ability of the economic unit to accomplish any distinct or different activities from its competitors (JATMIKO, 2021). Also, the competitive advantage is that technology, skill, or distinguished resource that enables the economic unit to produce values and benefits for customers that exceed what competitors offer because it achieves more values and benefits for them (Wang, 2021). It can be defined as the ability of the economic unit to formulate and implement strategies that put it in a better position in relation to other economic units operating in the same activity, and it is achieved through the best utilization of the technical, material, financial and organizational capabilities and resources in addition to the capabilities, competencies, knowledge and other capabilities that the unit enjoys, and it is related Achieving it in two basic dimensions: the perceived value of the customer and the ability of the economic unit to achieve excellence (Knudsen,2021,363). The sustainable competitive advantage can also be described as the means by which the economic units can obtain a competitive position in the markets by providing the best products and services in the right quantity and quality and at the right time. Sustainable competitive advantage can be defined as an element of superiority of the economic unit in exploiting its sources of strength and following innovative strategies to add value to its products that competitors did not reach.

Characteristics of sustainable competitive advantage mentioned by following: (Jenab, & Moslehpour,2016), (Radziwill, & Benton.2017), (Haseeb, 2019) for determined the needs and desires of the customer and provide an important support that contributes to the success of the business. Harmony between the resources of the economic unit and the opportunities in the environment. It also provides guidance and motivation to all economic entities.

The sustainable competitive advantage has differed dimensions, according to the opinions of some thinkers and researchers, and mentioned most important trends as follows (Cremer,et al.,2022) (TEGUH, et al.,2021):

Cost: an important issue for firm's costs savings through the efficient using of resources and production capacity, the purpose of maintaining cost competitiveness, and creating innovative ways to maintain the quality of products and services for customers without increasing their costs.

Quality: It refers to providing products or services in a distinctive way that suits the needs of customers, and adopting a system that guarantees the continuity of high quality.

Flexibility: The extent or dimension that measures the rapid response to customer requirements by changing the ability of those units to bring about a change in operations to other methods.

Delivery: The time of providing the service or delivery in a timely manner is considered one of the most important dimensions of sustainable competitive advantage because it determines the level of service quality, and the resulting costs of service provision operations.

Creativity: it is a distinguishing skill with high technology, which is the cornerstone of competition and achieving a sustainable competitive advantage, so that it is a unique value that is difficult to emulate.

Market share: The greater the economic unit's share in the market, the stronger its competitive position, the greater the potential returns on future investment, and the greater the future long-term competitive advantage.

https://doi.org/10.56294/sctconf2024670

Customer (sustainability): The customer satisfaction is priority because it is a primer goal of the firms, and thus customers will give more value to its products, which leads to excellence.

The cyber security is contributed to the promotion of sustainable competitive advantage. Some economic entries have realized that the only factor that keeps them in the race for leadership and achieves a sustainable competitive advantage for them is the interest in the basic requirements for building them, the most prominent of which is the interest in cyber security, which has recently become an important and high place in the interests of Various countries and economic units, as a result of the privileges achieved in raising competitive capabilities, and by relying on how to research and address information security, which has become an integral part in the field of security sciences, and reviewing deficiencies in information security leakage or violations that the economic unit is exposed to because it is linked to achieving a competitive advantage Sustainable in the field of aviation service at all airports until the information security of airports is achieved from the danger of terrorism and the threats posed by the revolution of contemporary information technology, and fortify it so as not to make it vulnerable to intrusions, violation of privacy and restriction of public freedoms (Ehioghiren, et al. 2021), (Rabiser& Zoitl,2021).

METHOD

Research Approach: this study follows a survey research design approach to measure the effect of cyber security cost of the sustainable competitive advantage and controls on cyber security within Iraqi firms.

Population and sample: the population for the study consists of 350 accountants, mangers, tax managers, practitioner assistances, and internal auditors in Iraqi airports. In determining the sample size for the study, the researchers used the judgmental sample to pick (6) airports around Iraq. The total number of officers was 250; the researcher used the questionnaire to obtain primary data.

Questionnaire distribution: the questionnaire was designed in a structured form and were randomly distributed made up of general questions of two research questions sections as follows; first section consist (24) questions for cyber security costs categories and second section for the sustainable competitive advantage has (28) questions to be measured via 5-point Likert scale according to the four hypotheses. The questionnaire was restricted with the responses made of (Strongly agree (SA) agree (A) undecided (U) strongly disagree (SD) and disagreed (D)). Out of the 250 copies of questionnaires distributed, only 232 questionnaires were usable, representing a 93 % overall response rate.

Data analysis technique: the 232 questionnaires were processed, and the hypotheses formulated for the study were tested with F-test statistics using the Eviews software package version 12. Using Eviews, 1 % is considered a normal significant level. F- Test statistic was used to test the hypotheses formulated. The decision was that if F-value is equal or higher than the scheduled value, there is a significant interaction effect.

RESULTS AND DISCUSSION

Data Analysis and results the data collected were analyses as show in the tables. Test of hypothesis one H1: There is affect of cyber security costs related to the property and information on sustainable competitive advantage in Iraqi airports. Test of hypothesis two H2: There is effect of cyber security costs related to the theft of confidential information and improving the procedures on sustainable competitive advantage in Iraqi airports. Test of hypothesis three H3: There is effect of cyber security costs related to external support on sustainable competitive advantage in Iraqi airports. Test of hypothesis four H4: There is effect of cyber security costs related the development of information systems on sustainable competitive advantage in Iraqi airports. This hypothesis is tested with the data in table 4 using F- test statistics.

Preliminary analysis: Descriptive statistics from a sample for cyber security costs categories and sustainable competitive advantage are presented in Table 1. The mean of property and information is 4,193 (median 4,166). The mean of theft of confidential information and improving the procedures is 4,056 (median 4,0). The mean of external support is 3,973 (median 4,0). The mean of development of information systems is 4,071 (median 4,0). On average, the sustainable competitive advantage, mean is 3,966 (median is 4,0).

Test of stationarity: The stationary test is a good econometric practice to restricted co-integrating vectors for determining the long relationships. A Table reports the results of Augmented Dickey-Fuller tests. All variables are rejected the null hypothesis of a unit root that the empirical variables are stationary. The next test for co-integration applying the Johansen technique in four separate models.

As expected, all empirical variables were negative ((0,04 = -1,179, $p<0$), and the results from the test for existence or not of a unit root in the log levels of our variables. The statistical values are higher than the critical values rejecting the null hypothesis of the unit root. Therefore, all our variables are integrated.

Co-integration tests: the test of Johansen trace and maximum eigenvalue statistics on co-integration for the empirical models are presented in Table 3.

The co-integration examination provides a natural setting for testing cross-variables relationships in permanent output movements. The cointegrating test explains that the relationship between cyber security

https://doi.org/10.56294/sctconf2024670

costs categories and sustainable competitive advantage is long- running, depend on the Johansen trace and maximum eigenvalue statistics are rejected the null hypothesis implies that there are co-integrating vectors at the 5 % level for the entire two-model variables (r≥0, r≥1 andr≥2).The results of co-integration is accepted all models in the full estimates of co-integrating vectors at the 5 % level. This suggests allows to examine the hypotheses by regression analysis in the next table.

Table 1. Description statistics

Variable	Mean	Standard Dev.	Median	Maximum	Minimum
property and information	4,193	0,508	4,166	5,0	2,66
theft of confidential information and improving	4,056	0,571	4,0	5,0	2,833
procedures external support	3,973	0,618	4,0	5,0	2,166
development of information systems	4,071	0,564	4,0	5,0	2,233
sustainable competitive advantage	3,966	0,564	4,0	5,0	2,250

Table 2. Results of Augmented Dickey-Fuller Tests: stationary analysis

Variable	Coefficient	Standard Error	Critical value	t statistics (Prob.*)
Property and information	-0,954 (-)	0,06	(-3,458)	-14,43*** (0,000)
Theft of confidential information and improving	-0,982 (-)	0,06	(-3,458)	-14,798*** (0,000)
Procedures external support	-0,886 (-)	0,06	(-3,458)	-13,50*** (0,000)
Development of information systems	-0,919 (-)	0,06	(-3,458)	-13,934*** (0,000)
Sustainable competitive advantage	-1,094 (-)	0,06	(-3,458)	-16,631*** (0,000)

Table 3. Results from Johansen Co-integration Tests

Model	Null	Eigenvalue	Trace Statistics	Max. Eigen. Stat.
Property and information with sustainable competitive advantage	None *	0,24	112,2*** (0,000)	64,5*** (0,000)
	At most 1 *	0,18	47,6*** (0,000)	47,6*** (0,000)
Theft of confidential information and improving the procedures with sustainable competitive advantage	None *	0,20	101,02*** (0,000)	53,4*** (0,000)
	At most 1 *	0,19	47,2*** (0,000)	46,2*** (0,000)
External support with sustainable competitive advantage	None *	0,19	94,8*** (0,000)	48,6*** (0,000)
	At most 1 *	0,18	46,2*** (0,000)	46,2*** (0,000)
Development of information systems with sustainable competitive advantage	None *	0,20	90,9*** (0,000)	52,9*** (0,000)
	At most 1 *	0,15	37,9*** (0,000)	37,9*** (0,000)
Property and information, Theft of confidential information and improving the procedures, External support ith sustainable competitive advantage, Development of information systems , and sustainable competitive advantage	None *	0,26	271,2*** (0,000)	70,9*** (0,000)
	At most 1 *	0,24	200,09*** (0,000)	63,5*** (0,000)
	At most 2 *	0,23	136,7*** (0,000)	60,02*** (0,000)
	At most 3 *	0,17	67,5*** (0,000)	44,8*** (0,000)
	At most 4 *	0,13	31,7*** (0,000)	31,7*** (0,000)
Reject the null of no co-integration among empirical variables at the 5 % level.				

Numberical Examples : In this part, the study provide five numerical tests for relationships where there is influence, meaning the influence of four cyber security costs categories on sustainable competitive advantage, a test 232 is required to verify the statistical significance of this influence. In Table 4, a summary of the hypotheses with their acceptance or rejection is presented, Coefficients of cyber security costs categories positivity have affected sustainable competitive advantage including the p-value for the relationships among the constructs, as well as the regression test that confirms direct effect. As a result, the following five hypotheses were supported: H1, H2, H3, H4, and H5.

In model 1, cyber security costs of property and information influence on sustainable competitive advantage in airports (coefficient>0, p<0,01) ,(t-statistics 8,1), the adjusted R^2 is 22 %. Meaning, sustainable competitive advantage increase 0,52 % per 1 % increase in cyber security costs of property and information. Model 2

https://doi.org/10.56294/sctconf2024670

showed, cyber security costs of theft of confidential information and improving the procedures influence on sustainable competitive advantage in airports (coefficient>0, p<0,01) ,(t-statistics 10,05), the adjusted R^2 is 30 %. Meaning, sustainable competitive advantage increase 0,54 % per 1 % increase in cyber security costs of theft of confidential information and improving the procedures . In the case of external support, cyber security costs of external support influence on sustainable competitive advantage in airports (coefficient>0, p<0,01) ,(t-statistics 7,4), the adjusted R^2 is 19 %. Meaning, sustainable competitive advantage increase 0,40 % per 1 % increase in cyber security costs of external support. For model 4 , cyber security costs of development of information systems influence on sustainable competitive advantage in airports (coefficient>0, p<0,01) ,(t-statistics 9,02), the adjusted R^2 is 26 %. Meaning, sustainable competitive advantage increase 0,51 % per 1 % increase in cyber security costs of development of information systems . while on the model 5 presented the total effects of cyber security costs on sustainable competitive advantage, (coefficient 1>0, coefficient 2>0, coefficient 3>0, coefficient 4>0, p<0,05, p<0,01, p<0,05, p<0,05 respectively) ,(t-statistics 1,02, 3,03, 1,7, 2,5 respectively), the adjusted R^2 is 33 %. Meaning, sustainable competitive advantage increase 0,11 % per 1 % increase in cyber security costs of property and information, 0,28 % per 1 % increase in cyber security costs of theft of confidential information and improving the procedures , 0,5 % per 1 % increase **in** cyber security costs of external support, and 0,20 % per 1 % increase in cyber security costs of development of information systems.

Table 4. Estimated regression model and long run coefficient

Variable	Coefficient	Standard Error	T-ratio]prob[	Result
Intercept : model 1	1,7 (+)	0,27	6,4] 0,000 [***	Supported
cyber security costs of property and information	0,52 (+)	0,06	8,1] 0,000 [***	
Adjusted R^2	0,22			
F-value	66,4			
Significant level	0,000			
Intercept : model 2	1,75 (+)	0,22	7,8]0,000[***	Supported
cyber security costs of theft of confidential information and improving the procedures	0,54 (+)	0,05	10,05]0,000[***	
Adjusted R^2	0,30			
F-value	101			
Significant level	0,000			
Intercept : model 3	2,3 (+)	0,21	10,9]0,000[***	Supported
cyber security costs of external support	0,40 (+)	0,05	7,4]0,000[***	
Adjusted R^2	0,19			
F-value	55,04			
Significant level	0,000			
Intercept : model 4	1,8 (+)	0,23	8,1]0,000[***	Supported
cyber security costs of development of information systems	0,51 (+)	0,05	9,02]0,000[***	
Adjusted R^2	0,26			
F-value	81,2			
Significant level	0,000			
Intercept : model 5	1,2 (+)	0,27	4,7]0,000[***	Supported
cyber security costs of property and information.	0,11 (+)	0,09	1,2]0,022[**	
cyber security costs of theft of confidential information and improving the procedures .	0,28 (+)	0,09	3,03]0,002[***	
cyber security costs of external support.	0,05 (+)	0,06	1,7]0,043[**	
cyber security costs of development of information systems.	0,20 (+)	0,08	2,5] 0,014 [**	
Adjusted R^2	0,33			
F-value	29,4			
Significant level	0,000			

Significant indicate *, **, *** at the 1 %, 5 %, 10 % level respectively.

DISCUSSION

This study presented a plan of the 6 airports with 232 employers in the Cyber security Framework to the four categories of costs (property and information, theft of confidential information and improving the procedures, external support, and development of information systems). The value of measuring costs of cyber security in terms of sustainable competitive advantage lies high in the levels themselves, and more in how the values relate to one another, change over time, and change in response to changes in strategy, firm, or cyber security investments. The primary limitation of this study is that the practical applicability must be assessed through future work on a broad scale in multiple countries and case studies.

Based on this finding, the paper became apparent that the sustainable competitive advantage does not

distinguish among the four categories of cyber security costs, and this is an important for managing the costs of cyber security - unless the entities find a simpler plan to cyber security cost model, and to track cost of rework. Furthermore, there are changes in the sustainable competitive advantage that should be segmented in cost accounting systems to reflect whether those tasks are being performed as fit. Companies may also wish to customize the plans to better performance with their unique systems, structures, and work processes.

CONCLUSIONS

In the extend of information technology, cyber security has a critical role. Protecting information has become challenging tasks. Cyber security comes to mind is risk, development, and competitiveness which are on the rise at the business environment. This study examines the positive influence between the cyber security costs and sustainable competitive advantage, as well as interesting and implementing, in airports. Testing modeling and co-integration were introduced; the definition of the cost cyber security was modified to mean short-run expectations combined with long-run improvement. The last approach which requires separating currency expectations from appreciations and using a non-linear cost asymmetry model. This method also allows determining if cyber security cost has positive effects via managerial decisions of sustainable competitive advantage. This approach may still be useful for related accounting systems with cyber security operations to sustainable competitive advantage. Airports need cyber security in order to provide its services with high quality via adopting customer satisfaction and increase the market share. It seems that any damage from cybercrime to airport security will cause higher costs than those resulting from natural disasters. The results revealed that the evidence of short-run and long-run cyber security costs effects significantly were established in Iraqi airports. Finally, cyber security costs revealed that while managerial decisions against the sustainable competitive advantage have favorable effects on the firm position.

REFERENCES

1. Aleksey Savkin, “Cybersecurity Scorecard with Key Performance Indicators for Data Security and Data Protection”, BSC Designer, September 25, 2021,

2. Antczak, J. (2020). Costs of Cyber-Security in a Business Entity. Edukacja Ekonomistów i Menedżerów, 55(1), 82-94.

3. Bulto, L., & Kant, S. (2023). Total Quality Management Integration With Six Sigma for Operational Success of a Project. Partners Universal International Research Journal, 2(2), 156-168.

4. Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. The Geneva Papers on risk and insurance-Issues and practice, 47(3), 698-736.

5. Ehioghiren, E. E., Ojeaga, J. O., & Eneh, O. (2021). Cyber security: the perspective of accounting professionals in Nigeria. Accounting and taxation review, 5(2), 15-29.

6. Ghelani, D. (2022). Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. Authorea Preprints.

7. Haseeb, M., Hussain, H. I., Kot, S., Androniceanu, A., & Jermsittiparsert, K. (2019). Role of social and technological challenges in achieving a sustainable competitive advantage and sustainable business performance. Sustainability, 11(14), 3811.

8. Hejase, H. J., Fayyad-Kazan, H. F., Hejase, A. J., & Moukadem, I. A. (2021). Cyber security amid COVID-19. Computer and Information Science, 14(2), 1-10.

9. JATMIKO, B., Udin, U. D. I. N., RAHARTI, R., LARAS, T., & ARDHI, K. F. (2021). Strategies for MSMEs to achieve sustainable competitive advantage: The SWOT analysis method. The Journal of Asian Finance, Economics and Business, 8(3), 505-515

10. Jenab, K., & Moslehpour, S. (2016). Cyber Security Management: A Review. Business Management Dynamics, 5(11)

11. Knudsen, E. S., Lien, L. B., Timmermans, B., Belik, I., & Pandey, S. (2021). Stability in turbulent times? The effect of digitalization on the sustainability of competitive advantage. Journal of Business Research, 128,

360-369

12. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186.

14. Rabiser, R., & Zoitl, A. (2021). Towards mastering variability in software-intensive cyber-physical production systems. Procedia Computer Science, 180, 50-59.

15. Radziwill, N. M., & Benton, M. C. (2017). Cybersecurity cost of quality: Managing the costs of cybersecurity risk management. arXiv preprint arXiv:1707.02653

16. Radziwill, N. M., & Benton, M. C. (2017). Cybersecurity cost of quality: Managing the costs of cybersecurity risk management. arXiv preprint arXiv:1707.02653.

17. Romanowski, S.; (2016). Examine the costs and causes of cyber incidents. Cyber Security Journal, 2(2), 121-135

18. Singh, U., & Singh, P. (2022). Managing Cyber Security. Journal of Management and Service Science (JMSS), 2(1), 1-10.

19. TEGUH, S., HARTIWI, P., RIDHO, B. I., BACHTIAR, S. H., SYNTHIA, A. S., & NOOR, H. A. (2021). Innovation capability and sustainable competitive advantage: An entrepreneurial marketing perspective. The Journal of Asian Finance, Economics and Business, 8(5), 127-134

20. Venkatachary, S. K., Prasad, J., & Samikannu, R. (2017). Economic impacts of cyber security in energy sector: A review. International Journal of Energy Economics and Policy, 7(5), 250.

21. Wang, H., Ko, E., Woodside, A., & Yu, J. (2021). SNS marketing activities as a sustainable competitive advantage and traditional market equity. Journal of Business Research, 130, 378-383.

22. Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. The Geneva Papers on risk and insurance-Issues and practice, 47(3), 698-736.

23. Rabiser, R., & Zoitl, A. (2021). Towards mastering variability in software-intensive cyber-physical production systems. Procedia Computer Science, 180, 50-59.

24. Radziwill, N. M., & Benton, M. C. (2017). Cybersecurity cost of quality: Managing the costs of cybersecurity risk management. arXiv preprint arXiv:1707.02653.

25. Jenab, K., & Moslehpour, S. (2016). Cyber Security Management: A Review. Business Management Dynamics, 5(11) Muravskyi, V. (2021). Accounting and Cybersecurity.

26. Singh, U., & Singh, P. (2022). Managing Cyber Security. Journal of Management and Service Science (JMSS), 2(1), 1-10.

27. Bulto, L., & Kant, S. (2023). Total Quality Management Integration With Six Sigma for Operational Success of a Project. Partners Universal International Research Journal, 2(2), 156-168.

28. Ehioghiren, E. E., Ojeaga, J. O., & Eneh, O. (2021). Cyber security: the perspective of accounting professionals in Nigeria. Accounting and taxation review, 5(2), 15-29. Antczak, J. (2020). Costs of Cyber-Security in a Business Entity. Edukacja Ekonomistów i Menedżerów, 55(1), 82-94

FINANCIACIÓN

Los autores no recibieron financiación para el desarrollo de la presente investigación.

CONFLICTO DE INTERESES

Los autores declaran que no existe conflicto de intereses.

CONTRIBUCIÓN DE AUTORÍA

Conceptualización: Sahar Yass AL-Asady, Inaam Mohsin Almusawi, Karrar Abdulellah Azeez.
Curación de datos: Sahar Yass AL-Asady, Inaam Mohsin Almusawi, Karrar Abdulellah Azeez.
Análisis formal: Sahar Yass AL-Asady, Inaam Mohsin Almusawi, Karrar Abdulellah Azeez.
Adquisición de fondos: Sahar Yass AL-Asady, Inaam Mohsin Almusawi, Karrar Abdulellah Azeez.
Investigación: Sahar Yass AL-Asady, Inaam Mohsin Almusawi, Karrar Abdulellah Azeez.
Metodología: Sahar Yass AL-Asady, Inaam Mohsin Almusawi, Karrar Abdulellah Azeez.
Supervisión: Sahar Yass AL-Asady, Inaam Mohsin Almusawi, Karrar Abdulellah Azeez.
Validación: Sahar Yass AL-Asady, Inaam Mohsin Almusawi, Karrar Abdulellah Azeez.
Visualización: Sahar Yass AL-Asady, Inaam Mohsin Almusawi, Karrar Abdulellah Azeez.
Redacción – borrador original: Sahar Yass AL-Asady, Inaam Mohsin Almusawi, Karrar Abdulellah Azeez.
Redacción – revisión y edición: Sahar Yass AL-Asady, Inaam Mohsin Almusawi, Karrar Abdulellah Azeez.

https://doi.org/10.56294/sctconf2024670