# THE EFFICIENCY AND EFFECTIVENESS OF THE CYBER SECURITY IN MAINTAINING THE CLOUD ACCOUNTING INFORMATION

**Salam Nawaf Almomani, Aqaba University of Technology**
**Mohammad Shehab, The World Islamic Sciences and Education University**
**Mohannad Mohammad Al Ebbini, Ajloun National University**
**Almohannad Ali Shami, King Abdalazeez University**

## ABSTRACT

*The study is aimed to identify the effect of the Cyber security Efficient and Cyber security effectiveness on Cloud accounting information in Jordanian public shareholding companies from the point of view of Professors and Managers information security. To answer the problem of the study a questionnaire was developed and distributed to 125 Professors and 75 Managers information security. By testing the hypotheses of the study, there is a significant impact of the of Efficient and Cyber security effectiveness on Cloud accounting information. This corresponds to the fact that Cyber security Efficient and Cyber security effectiveness it increases Reliability of cloud accounting information and reflects on the outcome of Earnings.*

**Keywords:** Cyber Security, Cloud Accounting Information, Effectiveness, Efficiency.

## INTRODUCTION

Cyber security is a technology used to defend computers, mobile phones, servers, electronic systems, networks and data from unauthorized attacks. The term is used in various cases from business to mobile computing Anna & Erhan (2015). Jordan is considered one of the economically developing countries and off course it is not secured from the cyber-attacks. Fawzi-Otoom, Ghadeer, et al. (2019) Showed that Jordan was ranked eighth in the Arab world and 63rd at the world level in having one million attacks annually. He also stated that the commercial sectors in the world incur (400) billion dollars annually as a result of these cyber-attacks that target these sectors and that there are (90) million incidents annually related to cyber security, which is a natural result of the existence of gaps in the security of information, networks, processes and applications.

The Central Bank of Jordan has indicated that Jordan has witnessed a significant development in the field of the financial information technology and innovation as a result of Jordan's possession of an investment environment for supporting innovation and high demand for financial technology in the Jordanian market. As a result, the central bank of Jordan announced its support for the innovations and initiatives that use the modern international technologies specially those enhancing the accessibility to the digital financial services with ease, efficiency and security taking into account the need to enhance and support the cyber (electronic) security of the financial service in general Sfeir (1966).

As a result of the increased interest of researchers and organizations that focus on cyber security, there is no doubt that some companies in light of their use of advanced technology, including cloud computing, are not immune to the risks of using cloud computing. Therefore,

www.manaraa.com

many companies have refrained from using the cloud computing because they do not trust using them for fear and concern of their financial data and information.

This might be attributed to their lack of trust in the efficiency and effectiveness of cyber security and its ability to maintain and recover information in case of a cyber-attack or natural disasters.

The problem of the study can be formulated as:

1. Is there any impact for the efficiency and effectiveness of the cyber security on maintaining the cloud computing information from the point of view of the university professors specialized in the information security?

2. Is there an impact for the efficiency and effectiveness of the cyber security on maintaining the cloud computing information from the point of view of the information security managers?

# RESEARCH HYPOTHESES

Based on the research problem, questions and previous studies, the research hypotheses were formulated as follows:

*H1 There is no impact for the efficiency and effectiveness of cyber security in maintaining the cloud computing information from the point of view of the University professors specialized in information security.*

*H2 There is no impact for the efficiency and effectiveness of the cyber security on maintaining the cloud computing information from the point of view of the information Security Managers.*

## Research Importance and Objectives

The main objective of this study is showing the efficiency and effectiveness of the cyber security in maintaining the cloud computing information. However the importance of this study to researchers lies in filling the theoretical framework gap while for corporations, the study shows them the importance and efficiency of cyber security in maintaining their information.

The organization of this review is as follows. Section 2 presents the related works. Then, the research methodology is described in Section 3. Section 3 shows experimental results and discussions. Finally, Section 5 presents Conclusions.

# LITERATURE REVIEW

## Cyber Security

There are many definitions for Cyber security. Alashqar, et al. (2012) stated that it is the activity that provides the protection to the human and financial resources linked to communication and information technologies, ensures the potential to reduce losses and damages in case of risks and threats, and allows for restoring the previous cases as soon as possible in order to keep the production wheel go on and so that damages would not turn into permanent losses.

Banga (2019) defined cyber security as the analysis, warning, reduction of the risk of exposure to cyber-attacks, and sharing information in order to take advantage of the networking information system. While al-Bar and Adnan-Mustafa & Khalid-Ali (2018) defined Cyber security as the sum of technical and administrative means used to prevent the unauthorized use, abuse, and recover of electronic information, communications and information systems for ensuring the continuity of the work of information systems and ensuring the protection, confidentiality and privacy of personal data and for protecting citizens. Based on the various definitions of the term, the re- searcher believes that cyber security is a group of technological regulations, rules and principles that can be used to protect the confidentiality of all financial,

administrative, legal and security information to mitigate the risk of cyber-attacks that will keep the security of the state and its social, economic and political entity.

The principle of cyber security work stems from the fact that it provides the protection of information by maintaining its integrity, condefintiality, and availability in addition to keeping the credibility, accountability, and validity of the information. Based on its work, it appeared that there is a difference between the efficiency and effectiveness of cyber security, as the Benzel (2011) reveals that its impact on the efficiency of cloud computing can be noticed through a range of key factors: The formation of multiple resources, the separation of data assets, and the use of external resources. This leads to increasing the quality of cloud computing by cyber security and increasing its importance regarding the effectiveness of cyber security. Facundo, Nadia, & Victor (2020), the authors stated that the effectiveness of cyber security depends on several factors that must be committed to and reviewed continuously to discover the loopholes through which information can be hacked and stolen. Table 1 shows the elements and risks of cyber security.

| Table 1 THE ELEMENTS AND RISKS OF CYBER SECURITY | | |
|---|---|---|
| Properties | Details | Source |
|  | Persons |  |
|  | Strategy | Mahatat (2021) |
| Elements | Process |  |
|  | Technology |  |
|  | Economic Risk | Al-Taleb, Saqib, Sujata (2020), Abdelkareem (2012) |
| Risk | Low Risk |  |
|  | Technology Risk |  |

## The Difference between Information Security and Cyber Security

The terms information security and cyber security are very similar; however, there are some differences between them. The information security is more comprehensive and general than cyber security where the latter is considered a branch or a field of the sciences of the information security. Furthermore, the information security is concerned with providing protection for systems and information by means and tools of pre-detection and facing threats. On the other hand, the cyber security focuses on the techniques, systems and strategies of defending computer systems and smart networks without paying attention to the means used as the encryption methods.

## The Efficiency and Effectiveness of Information

According to the Arab Society, p. 109 Mahatat (2021), the efficiency and effectiveness are two terms that are frequently used in the administrative accounting where each has a special meaning. Many definitions for the efficiency include that it is a set of qualities of processes indicating their ability in using the possible resources at the lowest possible cost for a specific goal.

The Arab Society, p. 315 Mahatat (2021) also defines it as the ratio between the amount of the resource planned and the resource actually used. Facundo, Nadia & Vıctor (2020), efficiency was defined as the optimal use of resources to achieve the best objectives; the efficiency is related to the productivity to determine the amount of addition in the value of each component of production. Efficiency is thus relative that it may rise or decrease, and therefore it is measured by the ratio of outputs to inputs or the ratio of utility to cost.

Based on the above, the researcher believes that efficiency is measured by the extent to which material and human resources are provided and used optimally for the purposes of achieving the objectives compared to the outputs or results achieved.

Regarding the effectiveness, Al-Dawi & Al-Sheikh (2010) believes that it is the ability to achieve the goals and reach the expected results," adding that the effectiveness is linked to the strategic objectives of the institution, and thus it is embodied in: the organization's ability to achieve its strategic objectives of growing sales and maximizing its profits." Therefore, the researcher believes that it is necessary to link the objectives with the outputs and compare the extent to which the establishment achieves its planned goals and identify the deviations to measure the effectiveness. Therefore, effectiveness is the degree of reaching towards the objectives.

### Cyber Security for Cyber accounting - Tool for the Digital Enterprise, Cristina (2019)

The global economic entities are facing growing transformation pressures - moving from product-driven business models to new models focused on creating and capturing different sources of new value. This article presents the future leader's perspective the impact of business digital transformation, but also the threats and vulnerabilities on managing accounting information system using Cyber security. The results show that the analytical cyber reveal that working in a digitized environment offer possibility for accountants to touch a field of cyber security.

### Communication Challenges in Cyber security, Marcia (2018)

Cyber-attacks are becoming a part of daily life, but navigating before, during, and after an attack is far from routine. With reputations on the line, cyber security is much more than an IT problem. Strategic communication across entire organizations is necessary to successfully navigate cyber security. This article outlines cyber security and cyber-attacks from a communication perspective and provides five cyber security communication challenges. Suggestions for further research are also included.

### The Evolution of Rules and Institutions in Cyber security: Cloud Computing and Big Data, Nir Kshetri (2016)

Cloud computing and big data are likened and equated to the Industrial Revolution. Their transformational natures are, however, associated with significant security and privacy risks. This chapter investigates how the contexts provided by rules and as well as formal and in- formal institutions affect the perceptions of privacy and security issues in big data and the cloud. It highlights the nature, origin, and implications of institutions in the context of these technologies. A goal of the chapter is also to gain insights into the mechanisms and forces that have brought about institutional changes in the cloud industry. Specifically, we investigate how contradictions generated at various levels by these technologies, the formation of dense networks and relationships and the changing power dynamics have triggered institutional changes. Since the current analysis of the causes and consequences of institutions and institutional change is mainly concerned with more established industries and markets, this chapter is expected to provide insights into institutions surrounding to this new and emerging technological development.

## The Impact of Foreignness on the Compliance with Cyber Security Controls, Waymond, Eyad Alhendi & Feixue (2019)

This study examines whether and how foreignness affects internal auditors' compliance with the International Standards for the Professional Practice of Internal Auditing (the Standards) from social and culture perspective. It demonstrates that foreignness, such as language and relational social capital, has a significant impact on auditors' compliance with the Standards, Especially with respect to cyber security, independence and objectivity, individual objectivity, and governance of the Standards. The Partial Least Squares Structural Equation Modeling (PLS-SEM) is used to analyze the survey data. This study highlights that external factors such as social capital affect the internal auditors' compliance with the Standards.

## Cyber Piracy in Cyberspace: The Escalating Threat to the Security of Countries, Shloush (2018)

The authors aimed to uncover the strategies and mechanisms that can be activated by the international systems to embody the international cyber security, the relation between the cyber piracy and making changes in the international cyber security environment, the impact of the cyber-attacks, including cyber piracy, on the emergence of new patterns of the international conflict while approaching the nature of these cyber-attacks, as well as the most new electronic weapons. Also, the paper aims to determine the international race witnessed by the world today from the international systems in the extent to which these cyber-attacks can be reduced in cyberspace.

## Cloud Computing

The term refers to the accessibility of software and data over the Internet any time at any place through any device that secures an internet connection. As for the term cloud computing, it is a description of the use of information technology that depends on the transfer of information, computing and storage space from the computer to the so-called cloud, which can be accessed through the web browser Karim (2019). Many researchers defined it as the technical servers connected together that are centrally managed through the use of local networks or internet, the so-called cloud, so that the accounting information and its programs are transformed from products into various accounting and financial services that are accessible to everyone and all those who request them in order to reduce time, costs and speed without the need for expensive equipment Al-Aydi (2019). Moreover, the cloud computing can also be defined according to Karim (2019), as the possibility of making the accounting information and processes available for 24 hours a day if there is any device that provides an internet connectivity.

## Cloud Computing Benefits

1. Saving time and money.
2. Providing physical comfort to the employee so he can work in any situation.
3. Contributing to the so-called green environment.
4. Achieving the efficiency of the accountant and the flexibility of the work.
5. The possibility of combining two jobs.

# RESEARCH METHODOLOGY

This section describes the methodology of the work which utilizes the Cyber security Efficient and Cyber security effectiveness to enhance the Cloud accounting information. Fig. 1 shows the Study framework/researchers design.
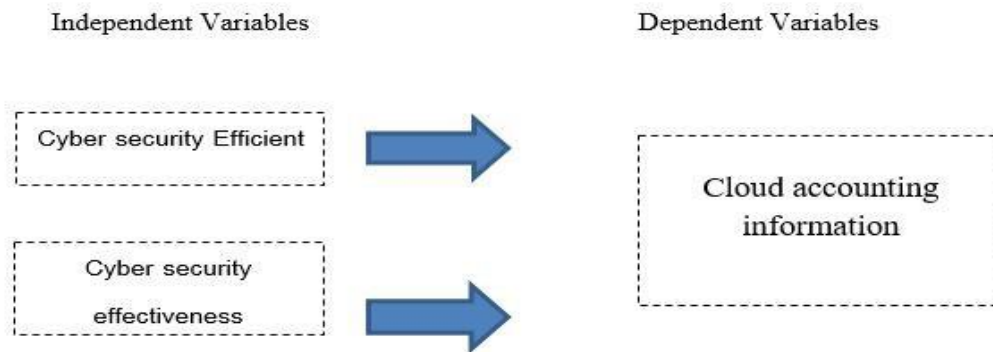


**FIGURE 1**
**STUDY FRAMEWORK/RESEARCHERS DESIGN**

## Population and Sample

The study dataset consists of the Cyber security Efficient and Cyber security effectiveness on Cloud accounting information in Jordanian public shareholding companies. To answer the problem of the study a questionnaire was developed and distributed to 200 University professors and 100 Managers information security, but only (250) questionnaires were retrieved therefore only 200 questionnaires were analyzed.

## Data Collection

In order achieve the aim of the study the descriptive and analytical approach was utilized. The study relied on two main sources for data collection: for the collection of secondary data: study utilized the previous studies, books periodicals scientific journals, and publications related to the subject of study. As for primary data, the study utilized the questionnaire designed to collect the data needed for the study.

## Goodness of Data

Before testing the research hypotheses, it is important that the data collected were checked for validity and reliability. The content validity of the instrument was ascertained by obtaining expert opinions from many lecturers in Jordanian universities.

# RESULTS AND DISCUSSIONS

It is necessary to reliability test to check for the reliability of the survey instrument. According to Saravanan & Rao (2007), the perfect measure of a concept needs more than one item. Hence, Cronbach's alpha (see Table 2) is considered an adequate indicator of the internal consistency and the reliability of the survey instrument and the test shows that the Cronbach's alphas range from 0.85 to 0.78, which exceed the minimum value of 0.70 to be acceptable. This

means that the instruments used to measure the variable were acceptable and the data were later used for further analyses.

| No. | Variables | Num. of Paragraphs | Cronbach's Alpha |
|---|---|---|---|
| 1 | Cyber security Efficient | 15 | 0.85 |
| 2 | Cyber security effectiveness | 15 | 0.87 |
| 3 | All Paragraphs | 30 | 0.86 |

Table 2 CRONBACH'S ALPHAS

## Normality Distribution

Fig. 2 shows the normal distribution of data, The results show the indicates that the data distribution was normal because the data Significance value is greater than 0.05 and the Kolmogorov- Smirnov test value is <5.
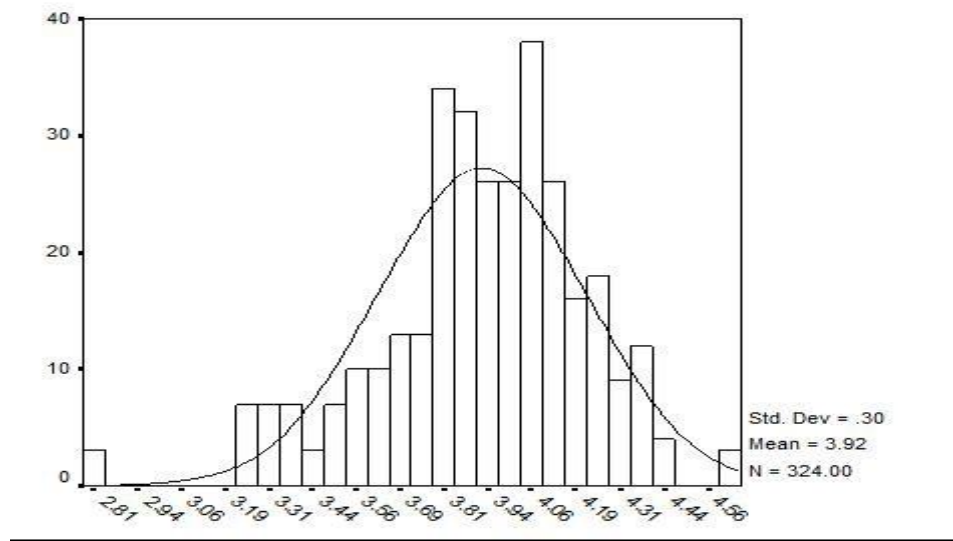


**FIGURE 2**
**NORMAL DISTRIBUTION OF DATA**

## Sample Characteristics

This section presents the demographic characteristics of the study sample Table 3 illustrates the result:

| Table 3 DEMOGRAPHIC CHARACTERISTICS | | | |
|---|---|---|---|
| **Category** | | **Frequency** | **Percentage (%)** |
| Education | Bachelor degree | 39 | 19.5 |
| | Master degree | 36 | 18 |
| | PhD | 125 | 62.5 |
| Total | | 200 | **100%** |
| Years of Experience | less than 5 | 6 | 3 |
| | 6 to 10 | 65 | 37.5 |
| | 11 to 15 | 62 | 31 |
| | 16 to 20 | 62 | 31 |
| | more than 20 | 5 | 2.5 |
| Total | | 200 | **100%** |
| Position | Professors | 125 | 62.5 |
| | Managers information security | 75 | 37.5 |
| Total | | 200 | **100%** |
| Specialization | Accounting | 75 | 37.5 |
| | Low | 25 | 12.5 |
| | information security | 100 | 50 |
| Total | | 200 | **100%** |

Demographic characteristics of the respondents presents that 19.5% of the sample held a Bachelor degree Those with a master's degree were only 18%, and the remaining either had PhD degree 62.5%.

In relation to experience, Table 1 shows that 37.5% of the sample had 6 to 10 years of work experience, and 31% had experience between 11-15 years and 31%had experience between 16-20 years, and the others either had less than 5 years of experience 3%, and more than 20 years of experience 2.5 %, regarding the specialization, the majority of the respondents majored in accounting 37.5%, Law 12.5% and information security 50%.

Finally, In relation to Position, Table 1 shows that 62.5% of the sample had Professors Position, and 37.5% Managers information security.

## HYPOTHESES TESTING

*HO1 There is no statistically significant at the (0.05) level for the Cyber security Efficient and Cyber security effectiveness on Cloud accounting information in Jordanian public shareholding companies from the point of view of Professors.*

| Table 4 REGRESSION BETWEEN CYBER SECURITY EFFICIENT AND CYBER SECURITY EFFECTIVENESS ON CLOUD ACCOUNTING INFORMATION IN JORDANIAN PUBLIC SHAREHOLDING COMPANIES. * SIGNIFICANT AT THE 0.05 LEVEL (MORE THAN: 0.05 = ACCEPT, LESS THAN: 0.05=REJECT) | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Samples** | **Variable** | **R** | **$R^2$** | **F** | **B** | **T** | **Sig t\*** |
| Managers information security | Cyber security Efficient | 0.2 | 0.04 | 10.55 | 0.22 | 3.55 | 0 |

| | Cyber security effectiveness | 0.33 | 0.108 | 7.32 | 0.33 | 2.56 | 0.005 |
|---|---|---|---|---|---|---|---|

Table 4 shows the results of the show the results of a regression between Cyber security Efficient and Cyber security effectiveness on Cloud accounting information in Jordanian public shareholding companies. And the results showed that there is a positively and significantly affects Cyber security Efficient and Cyber security effectiveness on Cloud accounting information and sample as a whole, the results of the study showed that the Cyber security Efficient and Cyber security effectiveness affects the Cloud accounting information from the point of view of Professors, where it was found that the value of (F) (10.550, 7.320, ) statistically significant values, as well as R values, which indicate a correlation between the independent variable and the dependent variable (0.20, 0.330, ), respectively, and $R^2$ (0.040, 0.108 ) respectively a value that explains the ability of the independent variable to influence the dependent variable at the confidence level of sig (0.00, 0.005).

*HO2 There is no statistically significant at the (0.05) level for the Cyber security Efficient and Cyber security effectiveness on Cloud accounting information in Jordanian public shareholding companies from the point of view of Managers information security.*

| Table 5 REGRESSION BETWEEN CYBER SECURITY EFFICIENT AND CYBER SECURITY EFFECTIVENESS ON CLOUD ACCOUNTING INFORMATION IN JORDANIAN PUBLIC SHAREHOLDING COMPANIES. * SIGNIFICANT AT THE 0.05 LEVEL (MORE THAN: 0.05=ACCEPT, LESS THAN: 0.05=REJECT) | | | | | | | |
|---|---|---|---|---|---|---|---|
| Samples | Variable | R | $R^2$ | F | B | T | Sig t* |
| Managers information security | Cyber security Efficient | 0.770 | 0.592 | 10.110 | 0.550 | 2.670 | 0.000 |
| | Cyber security effectiveness | 0.650 | 0.422 | 212.65 | 0.770 | 21.560 | 0.000 |

Table 5 shows the results of the show the results of a regression between Cyber security Efficient and Cyber security effectiveness on Cloud accounting information in Jordanian public shareholding companies. And the results showed that there is a positively and significantly affects Cyber security Efficient and Cyber security effectiveness on Cloud accounting information and sample as a whole, the results of the study showed that the Cyber security Efficient and Cyber security effectiveness affects the Cloud accounting information from the point of view of Managers information security, where it was found that the value of (F) (10.110, 212.650) statistically significant values, as well as R values, which indicate a correlation between the independent variable and the dependent variable (0.770, 0.650), respectively, and R * 2 (0.592, 0.422) respectively a value that explains the ability of the independent variable to influence the dependent variable at the confidence level of sig (0.000, 0.000).

| Table 6 | | | | | | | |
|---|---|---|---|---|---|---|---|
| REGRESSION BETWEEN CYBER SECURITY EFFICIENT AND CYBER SECURITY EFFECTIVENESS ON CLOUD ACCOUNTING INFORMATION IN JORDANIAN PUBLIC SHAREHOLDING COMPANIES. * SIGNIFICANT AT THE 0.05 LEVEL (MORE THAN: 0.05=ACCEPT, LESS THAN: 0.05=REJECT) | | | | | | | |
| All Samples | Variable | R | $R^2$ | F | B | T | Sig t* |
| Managers information security and Professors University | Cyber security Efficient | 0.66 | 0.4356 | 12.225 | 0.44 | 1.587 | 0 |
| | Cyber security effectiveness | 0.782 | 0.6115 | 215.551 | 0.79 | 21.56 | 0 |
| All Samples | | 0.89 | 0.792 | 145.21 | 0.69 | 11.8 | 0 |

Table 6 shows the results of the show the results of a regression between Cyber security Efficient and Cyber security effectiveness on Cloud accounting information in Jordanian public shareholding companies. And the results showed that there is a positively and significantly affects Cyber security Efficient and Cyber security effectiveness on Cloud accounting information and sample as a whole, the results of the study showed that the Cyber security Efficient and Cyber security effectiveness affects the Cloud accounting information from the point of view of Man- agers information security, where it was found that the value of (F) (12.225, 215.551) statistically significant values, as well as R values, which indicate a correlation between the independent vari-able and the dependent variable (0.660,0.782), respectively, and $R^2$ (0.4356, 0.6115 ) respectively a value that explains the ability of the independent variable to influence the dependent variable at the confidence level of sig (0.000, 0.000). And the point of view of sample as a whole the results showed that there is a positively and significantly affects the Cyber security Efficient and Cyber security effectiveness affects the Cloud accounting information that The R value 0.890 this mean there is a related between the Cyber security Efficient and Cyber security effectiveness and the Cloud accounting information, The $R^2$ of current study is 0.792 the (Cloud accounting information), with other factors remaining constant, The calculated F value is (145.210) and the significance level (Sig=0.000) is less than 0.05. Hence, the hypothesis is accepted.

## CONCLUSIONS

By testing the hypotheses of the study, there is a significant impact of the of Efficient and Cyber security effectiveness on Cloud accounting information. This corresponds to the fact that Cyber security Efficient and Cyber security effectiveness it increases Reliability of cloud accounting Information and reflects on the outcome of Earnings.

## RECOMMENDATION

Cyber security in some countries is a modern system, so it is through this research that the researcher recommends

– The role of cyber security must be strengthened in most companies in order to maintain accounting and cloud data and information, as it has proven to be the best way to preserve data without theft or penetration of systems.

– In the shadow of Corona "Coved 19", a lot of work could have been done, especially the office, if cyber security was used as a way to keep all financial data.

– The economy was greatly affected by the cessation of work due to the lack of confidence of many companies to operate remotely because their data are not protected in a high degree that does not allow penetration or theft like banks, so researchers recommend banks and major companies to review the security of their information so that they use cyber security, which enjoys a great degree of safety.

www.manaraa.com

– The researcher recommends conducting deeper studies, especially in developed countries with a strong economy in order to preserve their economy during natural and epidemic disasters.

## REFERENCES

Mahatat. (2021). https://www.mah6at.net/.

Al-Aydi, T.M. (2019). Evaluating the appropriateness of International Financial Reporting Standards ((IFRS) for measurement and reporting the revenues of cloud computing companies. *Journal of the Whole City of Science*.

Al-Barr, A.M., & Al-Muharbi, K.L. (2018). The future of cyber security in the kingdom of Saudi Arabia. In research presented to the Euro money Conference in Saudi Arabia, the Saudi Federation for Cyber Security and Programming, Riyadh-Saudi Arabia.

Al-Dawi, A.S. (2010). Analysis of the theoretical foundations of the concept of performance. *Researcher Journal*, (7), 2010.

Najla, A.T., Nazar, A.S., & Sujata, D. (2020). *Cyber threat intelligence for secure smart city*. ArXiv preprint arXiv: 2007, 13233.

Abdelkareem, M.A. (2012). A comparative study on Arabic pos tagging using quran corpus. In 2012 8th International Conference on Informatics and Systems, pages NLP–29. *IEEE*.

Karim-Hussein, A.W. (2019). Cloud accounting is a new horizon for organizing accounting work. *Journal of the Whole City of Science, 11*(1).

Alamuddin, B. (2019). The risks of cyber-attacks and their economic impact: A case study of the gulf cooperation council countries, journal of the Arab planning institute. *Development Studies*, (63).

Terry, B. (2011). The science of cyber security experimentation: The deter project. In Proceedings of the 27th Annual Computer Security Applications Conference.

Facundo, B., Nadia, R., & V´ıctor, D.F. (2020). An efficient met model-based method to carry out multi-objective building performance optimizations. *Energy and Buildings, 206*, 109576.

Anna, L.B., & Erhan, G. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications surveys & tutorials, 18*(2), 1153–1176.

Marcia, W.D. (2018). Communication challenges in cyber security. *Journal of Communication Technology, 1*(1), 43–60.

Kshetri, N. (2016). The evolution of rules and institutions in cyber security: Cloud computing and big data. In The Quest to Cyber Superiority. *Springer*.

Ahmed-Fawzi, O., Ghadeer, A.K., Maen, H., Rateb, J.S., & Haneen, H. (2019). Success factors importance based on software project organization structure. *Information, 10*(12), 391.

Waymond, R., Eyad, A., & Feixue, X. (2019). The impact of foreignness on the compliance with cyber- security controls. *Journal of World Business, 54*(6), 101012.

Rajagopal, S., & KSP, R. (2007). Measurement of service quality from the customer's perspective–An empirical study. *Total Quality Management and Business Excellence, 18*(4):435–449.

George, N.S. (1966). The central bank and the banking law of Jordan. *Middle East Journal, 20*(3):352–360.

Noura, S. (2018). Cyber hacking in cyber space: The rising threat to state security. *Journal of Babel Center for Humanitarian Studies, 8*(2).

Cristina stefˇanescu. (2019). Cyber security for cyber accounting.