Journal of Business Economics for Applied Research, Vol. (6), No. (2), Part (1):142-172
Doi: https://dx.doi.org/10.37940/BEJAR.2024.6.2.7

Journal of Business Economics for Applied Research
مجلة اقتصاديات الاعمال للبحوث التطبيقية
ISSN 2709-6475

The Impact of Diversity in Cybersecurity on the Protection of Future Accounting Information
An Analytical Study of the Opinions of a Sample of Professionals and Academics in Erbil City

Jarjees Mustafa Khdeer[(1)], Naseem Yousif Hanna[(2)], Dashti Khalid Hamadameen[(3)]

College of Administration and Economics, Salahaddin University-Erbil[(1)(2)(3)]
(1) Jarjees.khdeer@su.edu.krd, (2) naseem.allallo@su.edu.krd, (3) dashti.hamadameen@su.edu.krd

Key words:
Cyber Security, future accounting information, information security.

ARTICLE INFO
Article history:

Received	***23 Feb. 2024***
Accepted	***09 Mar. 2024***
Avaliabble online	***31 Dec. 2024***

*Corresponding author:
Jarjees Mustafa Khdeer
College of Administration and Economics
Salahaddin University-Erbil

Abstract:
The research aims to explain the role of Cyber Security in protecting future accounting information, given that it contains the company's future plans and strategies, which should be protected and not fall into the hands of competitors. To achieve the goal of the research, an electronic questionnaire was distributed to a sample of (132) individuals from professionals and specialized workers. In the field of accounting information systems, in addition to academic accounting in universities and institutes in the city of Erbil, and its results were analyzed by the statistical program (SPSS), and the research reached a number of conclusions, most notably that there is a statistically significant impact of diversity in Cyber Security in protecting future accounting information, and in Finally, the research made some recommendations, the most important of which is the need for companies to protect their future accounting information by setting complex passwords and not making company communications available to any third parties without a private encryption key, in addition to conducting a test to verify the extent to which applications meet security requirements.

Journal of Business Economics for Applied Research, Vol. (6), No. (2), Part (1):142-172
Doi: https://dx.doi.org/10.37940/BEJAR.2024.6.2.7

أثر التنوع في الأمن السيبراني على حماية المعلومات المحاسبية المستقبلية دراسة تحليلية لآراء عينة من المهنيين والأكاديميين في مدينة أربيل

أ.م.د. جرجيس مصطفى خضر
كلية الإدارة والاقتصاد
جامعة صلاح الدين-اربيل
Jarjees.khdeer@su.edu.krd

أ.م.د. نسيم يوسف حنا
كلية الإدارة والاقتصاد
جامعة صلاح الدين-اربيل
naseem.allallo@su.edu.krd

أ.م. دشتي خالد حمدين
كلية الإدارة والاقتصاد جامعة
صلاح الدين-اربيل
dashti.hamadameen@su.edu.krd

المستخلص

يهدف البحث إلى بيان دور الأمن السيبراني في حماية المعلومات المحاسبية المستقبلية نظرا لأنها تحتوى على خطط واستراتيجيات الشركة المستقبلية و التي ينبغي حمايتها وعدم وقوعها في ايدي المنافسين، ولتحقيق هدف البحث تم توزيع استمارة استبيان الكترونية على عينة مكونة من (132) فردًا من المهنيين والعاملين المتخصصين في مجال نظم المعلومات المحاسبية بالإضافة الى أكاديمي المحاسبة في الجامعات والمعاهد في مدينة أربيل، وتم تحليل نتائجها بواسطة البرنامج الإحصائي (SPSS)، وتوصل البحث إلى عدد من الاستنتاجات أبرزها أن هناك تأثير ذو دلالة إحصائية للتنوع في الأمن السيبراني في حماية المعلومات المحاسبية المستقبلية، وفي الأخير قدم البحث بعض التوصيات أهمها ضرورة قيام الشركات بحماية معلوماتها المحاسبية المستقبلية من خلال وضع كلمات مرور معقدة وعدم إتاحة اتصالات الشركة لأي طرف ثالث دون مفتاح تشفير خاص. بالإضافة إلى إجراء اختبار للتحقق من مدى تلبية التطبيقات للمتطلبات الأمنية.

الكلمات المفتاحية: الامن السيبراني، المعلومات المحاسبية المستقبلية، امن المعلومات.

1.Introduction : Today's world is witnessing a continuous change in various fields of economic activity, and the increasing practical and scientific development in those areas has led to an increase and exacerbation of the burdens and responsibilities placed on the shoulders of organizations, which gave information technology a necessity of our time and one of the main work tools, and as a result of this great boom that occurred in the means of communication and information networks, new risks and threats appeared in the business arena, which necessitated taking all available and possible means to enhance information security and protection, which is inevitable. To maintain the confidentiality of information through the existence of regulatory procedures to preserve this information, represented by Cyber Security (Mansour, 2021: 224), and on the other hand, the usefulness of future financial information has become widely recognized at the present time, and the demand for this information is increasing by many parties from the financial community, including current and prospective capital owners, credit lenders and others, and future financial information is used in many multiple fields, starting with companies that offer their securities From shares and bonds to the public for public subscription and companies seeking loans from banks and financing bodies, and ending with the uses of this future information in short-term internal project plans (budgets), long-term plans and others, and due to the importance of

protecting this accounting information, researchers have formed the idea of how to protect that information through types of Cyber Security.

1.1: The Research Problem:

There is no doubt that the issue of security and protection of accounting information is one of the most important issues in our current era, as the success of any company depends largely and clearly on the accounting information it possesses. We must take into account that this information and systems used by companies are exposed to risks from time to time. And the other, the reason for this is because it faces multiple types of information breaches and criminal activities that it is exposed to, such as disruption of services and destruction of property. Here, there must be security through which the company's future accounting information can be protected, which is Cyber Security. The research problem can be posed through the question. The main one is: What is the role of common types of Cyber Security in protecting future accounting information? The following sub-questions branch out from this main question:

1. Is Cyber Security important in protecting future accounting information?
2. Does Network Security (one of the types of Cyber Security) affect the protection of future accounting information?
3. Does Cloud Security (one of the types of Cyber Security) affect the protection of future accounting information?
4. Does Application OF Security (one of the types of Cyber Security) affect the protection of future accounting information?

1.2: The Hypothesis of the Research:

To answer the questions referred to in the research problem, the research depends on the following hypotheses:

1. Cyber Security is important in protecting future accounting information.
2. The Network Security, which represents one of the types of Cyber Security, affecting the protection of future accounting information.
3. The Cloud Security, which represents one of the types of Cyber Security, affecting the protection of future accounting information.
4. The Security of Applications, which represents one of the types of Cyber Security, affecting the protection of future accounting information.

1.3 : The Objective of research

The Main objective of this study was to investigating the role of diversity in Cyber Security in ensuring the protection of future accounting information, and from the main objective, four sub-objectives can be formulated as following:

1- To Investigate the importance of Cyber Security in the protecting future accounting information.
2- To Investigate the effect of Network Security in the protection future accounting information.

3- To Investigate the effect of Cloud Security in the protection future accounting information.
4- To Investigate the effect of Application OF Security in the protection of future accounting information.

1.4: The Importance of Research:

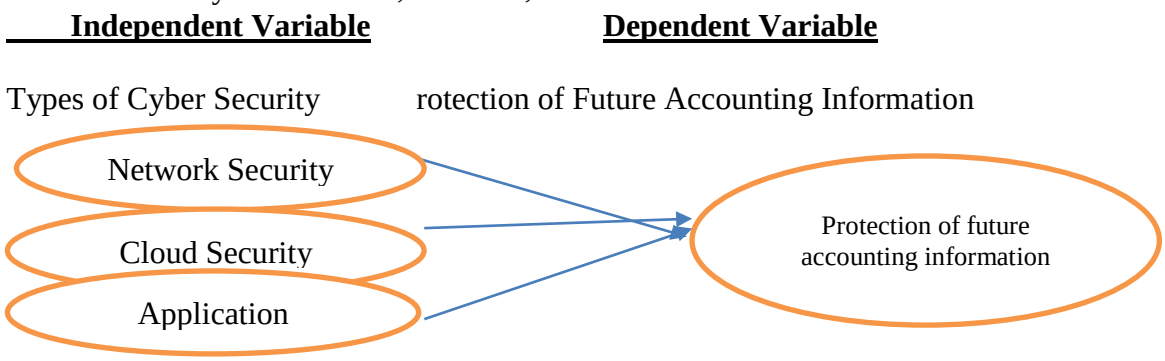
The importance of the research stems from the fact that it deals with one of the vital topics, which is Cyber Security, which is of great importance to many companies, as it serves as the basic firewall to protect various future accounting information for them, Any breach of this wall has devastating consequences for the company in terms of affecting the company's reputation and competitive advantage, and breach of future accounting information can affect corporate revenues due to non-compliance with information protection systems, so it is necessary for companies to adopt and implement a strong approach to Cyber Security.

1.5: Research Methodology: The researchers relied on the descriptive approach in formulating the theoretical side of the research, and at the same time the deductive approach was adopted in the practical side of it.

1.6: Research Framework: As shown below in Figure (1) the research model, which consists of research variables as follows:

Independent Variable. Cyber Security: It is a matrix of organizational, technical and procedural tools, and practices aimed at protecting computers, networks and data inside them from intrusions, damage, change, or disruption of access to information or services.

Dependent Variable. Future Accounting Information: It is the Accounting information related to future plans and forecasts that can be used and benefited from by shareholders, creditors, investors and others.



Figure(1) : The Research Framework

2 :Literature Review

2.1: The Concept of Cyber Security:

The number of Cyber Security incidents is increasing every year especially due to the increasing use of the internet, cloud computing and mobile devices, and Cyber Security incidents can lead to serious damage to hacked

companies in terms of treatment costs, fines and reputation, as Cyber Security incidents are complex and multifaceted events and their full effects may not always be realized immediately, for example, Equifax, a credit reporting agency, admitted on September 7, 2017, that hackers had hacked Information of more than 140 million individuals between May and July of the same year Hackers were able to exploit a vulnerability in their website and gain access to social security numbers, dates of birth, driver's license numbers and credit card information (Rosati, et al,2020: 4), this is done through cyberattacks that focus on obtaining certain economic benefits such as espionage, financial attacks, card fraud, information theft, phishing, network attacks, intellectual property theft and extortion. and others (Zadorozhnyi, et al,2021:37) These attacks are deliberate actions aimed at changing, disabling or destroying computer systems or networks, and as a result of the heavy losses caused by these attacks, Cyber Security has emerged, not only with the aim of defending or protecting against harmful computer attacks, but also in order to detect vulnerabilities in the system and work to fix them as soon as they are discovered, through which individuals, companies and systems are protected from cases of digital penetration, unauthorized access or threats. Serious security, which may affect the privacy of data and information, especially sensitive ones, as well as the management of the production process itself, especially since industries of all kinds are now closely related to technology, and in today's world Cyber Security may be the most important challenge facing the accountant according to (AICPA) (Ehioghiren, et al,2021: 16)

When reviewing the literature on the subject of Cyber Security, we notice that there are different definitions of it, as it defined (SEC) as "the set of techniques, processes and practices designed to protect networks, systems, computers, programs, and data from attack, damage or unauthorized access" (Heroux and Fortin, 2020: 76).

It is also defined as "technologies, processes and controls designed to protect systems, networks and data from cyberattacks, reduce the risk of cyberattacks, and protect communities, companies and individuals from the unauthorized exploitation of systems, networks and technologies. (Haapamäki and Sihvonen, 2019: 812)

Cyber Security is defined as "the activity, process, ability or ability to protect and defend information and communication systems and the information contained therein against damage, unauthorized use, modification or exploitation" (Gao, et al., 2020: 3).

Researchers can define Cyber Security as a set of technologies to protect systems and networks from cyberattacks or unauthorized use.

2.2: The Importance of Cyber Security:

The importance of effective Cyber Security is highlighted by reducing the risk of Cyber Security breaches designed to protect society, individuals and businesses from unauthorized use of systems, networks and technologies (Asiri,2021: 110) and that an effective Cyber Security program is one that reduces the risk of cyber-attacks and incidents and protects everyone from misuse or unauthorized use of related systems, networks and technologies (Badawy, 2021: 6) The ability to resist intentional and unintentional threats, respond and recover, thus being free from the danger or damage caused by the disruption or damage of ICTs or due to the misuse of ICTs and requires the protection of networks, computers, programs and data from attack, damage or unauthorized access. As a result of the importance of Cyber Security in the reality of today's societies, many countries have made it a top priority, especially after cyber wars that have begun to manifest their manifestations. Among some major countries, in an explicit reference to the end of conventional wars in which heavy weapons were used, and the announcement of the beginning of new wars are cyber wars (Al-Zubaidi and Al-Tamimi, 2022: 8), and given the significant financial, reputational, and legal implications of high-level modern cyberattacks, reporting the Cyber Security risks faced by companies and how to manage these risks is becoming increasingly important for investors, governments, consumers, suppliers and other stakeholders to make the right decision. (Gao, et al, 2020: 3) It can be argued that the importance of Cyber Security lies in: (Kaao, 2020: 171)

1. Maintain the confidentiality and privacy of all digital documents and data.
2. Ensure the availability of continuity of the functioning and functioning of digital systems.
3. Provide the necessary protection for citizens and important infrastructure of the state.

2.3: Types of Cyber Security:

The various activities carried out by companies today are related to technology, and this makes the need urgent to protect all systems from some cases of unauthorized penetration or the so-called digital penetration, especially serious security threats that can affect the privacy of information and data, especially sensitive information, as threats negatively affect information. Threats aim to degrade the integrity, confidentiality and availability of information, as some threats are known and some unknown (Horne, et al,2016: 7) and therefore this impact may reflect negatively on the company and these protections are called information security or what is called cyber security, which is a form of Cyber Security. Cyber Security can be divided into three broad categories. First, Cyber Security protects the confidentiality of private information, second, it ensures that authorized users can access information in a timely manner, and third, Cyber Security

protects the accuracy, reliability and validity of information (Haapamäki and Sihvonen, 2019: 809), There are several types of Cyber Security, but the most common types are:

1. Network Security: The protection of information stored in social networking sites is necessary over time, as people put more information in different forms on social networks that can lead to unprecedented access to information by people who seek to harm others, and in this regard many social networking sites have provided security and privacy settings to enable the customer to protect his personal information from unwanted access by strangers or applications. For example, a Facebook subscriber can modify their security settings and identify the echoes audience in the network whose details, photos, posts, and other sensitive information they can see. Moreover, it also allows its users to either acknowledge or deny third-party applications access to their personal information, as many internal security measures of the system are equipped against spam, fake profiles, spammers, hackers, and others (Jain, et al., 2021: 2167).
2. Cloud Security: Cloud computing has become a prominent part of the IT industry as a result of the spread of computing and reliance on it to distribute information across different geographical areas and the resort of many people towards adopting cloud computing. Nowadays there are many cloud service providers that allow customers to host their applications and data on the cloud. However, the fear related to the security of this service is still a challenge for its users and thus prevents users from accessing its services, as security plays an important role in creating trust between the user and the cloud service provider, and therefore the service provider resorts to relying on technologies that will mitigate risks related to Cloud Security, including hybrid encryption, which combines the advantages of both symmetric and asymmetric encryption and others
3. Application Security: Application OF Security includes actions taken to improve an application's security, often by finding, fixing, and preventing vulnerabilities. Different technologies are used to cover security vulnerabilities at different stages of the application lifecycle such as design, development, deployment, upgrade and maintenance, and examples of application security, web applications, databases, mobile applications, etc., and actions in Application OF Security take the form of hardware, software, or procedures to identify or reduce security vulnerabilities (Arora, et al., 2017: 289).

2.4: The Concept of Future Accounting Information:

At the end of each year, companies issue certain reports that include information about the company, and this information may be historical, i.e. financial results about the previous period, relevant disclosures and future financial information (Kılıç and Kuzey,2018: 119). Future information

refers to expectations regarding the company's business that ultimately provides parties related to the company's activity with useful information about the company's future prospects, as these parties often ask the company's management about the company's future forecast in the sense that What will happen to the company in the future, and the reporting of future information includes information about the company's financial forecasts, such as forecasting revenues, cash flows and sales volume, along with it includes information about non-financial expectations such as factors that may affect the company's future performance for example risks, future commercial uncertainty, analysis and evaluation, agency relationship, operations, and relevant general information about the company, the company's annual reports are one of the best means of delivering This information is for interested users in which future information is presented (Alkhatib,2017:35), and in general there are three categories of users of future financial information namely management, capital markets and ordinary users, management may request any kind of future accounting information necessary to make decisions such as evaluation of financing alternatives, acquisition of plant and equipment, development or cancellation of the production line, acquisition or sub-divestiture. In addition, entities that are large providers of capital (large suppliers, banks, investment groups and others) can negotiate investment terms and determine the provision of certain future financial information. In fact, the trend in negotiated capital markets has been to focus more on future financial information, and ordinary users are those who have no influence or authority over the company to obtain it and who use it for the purposes of monitoring the company's activity (Olson, 2011: 56).

He defined future accounting information as information about the company's current plans and future forecasts that enable investors and others to estimate the future performance of the company, which includes financial and non-financial information (Rajab, 2016: 383).

It was also defined as "information that is not disclosed in the basic financial statements of current plans and future forecasts that enable investors and others to estimate the future performance of the company, and the disclosure of future information may include non-financial information about the risks that may surround the company (Hussein, 2021: 105).

It was also defined as "information based on assumptions about future events and the company's reaction to them, which is by nature highly subjective, and its preparation requires the exercise of a great deal of personal judgment (Sabsby, 2011: 41).

Therefore, researchers can define future accounting information as that information about the current plans and future forecasts of the company,

which includes financial and non-financial information and is subject to high personal judgment by nature.

2.5: The Importance of Future Accounting Information:

There is an importance for reporting future accounting information by companies, it helps the user to understand the management's vision for the future and its plans for the company and the financial implications of these plans and the plans depend on key assumptions about the factors and conditions necessary for the success of those plans and the disclosure of those assumptions is important to investors because it provides a future vision of the opportunities and risks that the company will face, and this information is beneficial to management and reduces credit risk to the lender. Although it is important to disclose management plans, some users may prefer their own expectations as more objective. Estimates of future financial performance are inherently inaccurate and management may tend to be overly optimistic. The report also confirmed in the section on disclosure of information about the company that users also need basic information about the company that provides users with a mental image of the company's work (Rajab, 2016: 384), in addition to that, increasing the level of disclosure of such information leads to transparency of information and ultimately reduces the costs of indebtedness (Khankahdani, et al, 2021: 114), and in general the importance of reporting future accounting information is: (Hussein, 2020: 13)

1. Reporting forward accounting information is valuable in improving the ability of financial markets to anticipate future changes in profits, cash flows, operating performance indicators of companies, and future capital expenditures, providing reliable information that financial analysts rely on to improve their expectations of the company's future financial performance.
2. The credibility of publishing earnings forecasts increases when backed up by the disclosure of future statements.
3. Reporting future accounting information affects securities prices and investor decisions, as the share price in the capital markets responds more than the results of operations from historical revenues and profits, and share prices can be predicted more accurately, and this disclosure is one of the strategies to reduce conflicts with shareholders and an administrative effort to convince shareholders to focus on the future growth of the company, which increases its value.

2.6: Motives for Reporting Future Accounting Information:

There are many motives and reasons for the purpose of reporting future financial information, the most important of which are the following: (Khader et al., 2022: 561)

A. Increase the value of the company: The reporting of future accounting information ultimately leads to an increase in the company's value

(Khankahdani, et al, 2021: 114), as this information indicates the achievement of future profits that will lead to an increase in the value of the company by increasing the demand for its shares, and thus an increase in the market value of the company's shares.

B. Reducing information asymmetry: Reporting on future financial information will reduce information asymmetry and improve the decision-making process and thus improve external financing opportunities as well as reduce its cost, as companies reporting future accounting information will reduce information inconsistency between companies and thus can support interested parties in making better investment decisions (El-Deeb & Elsharkawy, 2019: 4)

C. Attracting new capital: Reporting future financial information is one of the important tools used by management to obtain new sources of funding by having a good reputation for the company among investors and increasing the degree of confidence in it. (Khader et al., 2022: 561)

d. Cost of capital reduction: Lower cost of capital is associated with the expansion of voluntary disclosure and the quality of profits, and future reporting reduces future uncertainty and thus reduces the risk that leads to a reduction in return. (Khader et al., 2022: 561)

2.7: Cyber Security and Protection of Future Accounting Information:

High-profile Cyber Security incidents in public companies have increased the sensitivity of investors to such incidents and increased demand for information about corporate Cyber Security risk management programs, and Cyber Security incidents have been defined as any event that violates the confidentiality of the origin, integrity or availability of information, as such Cyber Security incidents may consist of different types of events such as malware, ransomware, denial of service attacks or fraud when using credit cards or even human error, what Missing records and the direct and indirect costs associated with them make detecting such incidents a complex process (Metwally and Gharib, 2022: 265), and companies can protect their future accounting information by strengthening the types of Cyber Security as follows:

1. Network Security : Network Security is a set of procedures during which maximum protection of information and data in networks can be provided from all risks that threaten them, by providing the necessary tools and means to protect information from internal or external risks, as companies can protect their future accounting information by setting complex passwords and on more than one stage to access that information, in addition to restricting the granting of permission to enter the network with one trusted accountant or officials in The senior management of the company as well as providing maximum protection of information in

networks in order to avoid risks that may be inflicted by hackers or competitors of the company.

2. Cloud Security : Cloud Security is a complete set of technologies, protocols and best practices that protect cloud computing environments and applications that run in the cloud and the data saved in them, and since cloud computing is now used by many large companies, Cloud Security is a vital part of corporate Cyber Security, and companies can protect their future accounting information that has been stored in the cloud by ensuring that there is no unauthorized access to the cloud through other networks along with securing End-to-end encryption of all future accounting information uploaded to the cloud, so that the company's communications are not made available to any third parties without the company's encryption key, as well as protecting all devices used by the company to access future accounting information including smartphones and tablets.

3. Application OF Security : Application OF Security includes actions taken to improve the security of an application often by finding, fixing and preventing security vulnerabilities, keeping confidential information safe and secure, reducing risks from both internal and external sources, protecting sensitive information from leaks, and companies can protect their future accounting information here by conducting a test to verify the extent to which applications meet security requirements, as well as conducting a review of settings, immunization and update packages before launching and launching any application, as well as filling the gaps Security in Application OF Security by the company.

3: Results and Discussion

3.1: Description of Search Variables: The researchers coded the research variables, which include the research axes, represented by the axis of "types of Cyber Security", where the aforementioned axis was coded with the symbol (X), which is measured by its three dimensions, represented by "Network Security, Cloud Security, application security", which was coded as the three dimensional phrases as follows: (X1.1-X1.6), (X2.1-X2.6), (X3.1-X3.6)" and respectively, knowing that each of the three dimensions was measured using six phrases. The three dimensions are coded with X1, X2 and X3, respectively. As for the second axis, represented by "the importance of Cyber Security in protecting future accounting information", the aforementioned axis was coded with the symbol (Y), while its phrases were coded with codes from (Y1) to (Y7), meaning that they were measured by seven phrases or questions. In order to obtain the opinions and answers of the respondents about the axes and dimensions of the study mentioned above, the researchers used the five-point Likert scale, whose value ranges from (one degree = 1), which represents an answer (I do not strongly agree)

to (five degrees = 5), which represents (strongly agreed) as a means of collecting primary data about the respondents, where the questionnaire was distributed randomly to a sample of the research community, which includes academics, professionals and those covered by the subject of the study through the (Google form) platform, where 132 respondents filled Questionnaire Form, and then the ready-made statistical program "Statistical Package for Social Sciences - SPSS" was used in order to analyze opinions and answers, as well as reach the objectives of the research and test the hypotheses that came out of it.

3.1 Description of Personality Variables:

3.1.1: Distribution of Respondents According to Job Qualification: For the purpose of distributing the respondents' members according to the job qualification of academics and professionals, Table (1) was relied upon, through which it became clear that the majority of the respondents participated in the academic category, with a participation rate of (%78.79), while the rest were professionals who work in the field of accounting information systems, and their percentage was (21.21%) among the research sample.

Table 1: Distribution of Respondents According to Job Qualification

Variable classes	Frequency	Percentage
Academy	104	%78.79
Professional	28	%21.21
Total	132	%100

Source: Prepared by researchers based on the results of statistical analysis

3.1.2: Distribution of Respondents According to Academic Qualification : Through Table (2), which represents the distribution of the sample members of the respondents according to qualification or educational achievement, where it was found that the majority was within the category that obtained a master's degree with a contribution rate of (%62.12), where it ranked first in terms of participation, followed by respondents with a degree (PhD) with a participation rate of (%30.30) and finally the participation by the respondents and those with a (bachelor's) degree was few, as their participation does not exceed ten cases and their contribution rate reached (%7.58).

Table 2: Distribution of Respondents According to Academic Qualification

Variable classes	Frequency	Percentage
PhD	40	%30.30
Master	82	%62.12

Bachelor	10	%7.58
Total	132	%100

Source: Prepared by researchers based on the results of statistical analysis

3.1.3: Distribution of Respondents According to Years of Experience: According to the table below, it was found that the majority had years of experience falling within the category of more than sixteen years, where the percentage of their contribution from the respondents was (%39.39), where it ranked first in terms of participation, followed by the category, which was their years of experience ranging between eleven and fifteen years, while in third place, the respondents came from within the category (6-10) years of service with a participation rate of (%24.24) and finally the participation was by the category, which had years of experience not exceeding five Few years with the participation of eight cases among the respondents, whose participation rate is (%6.06).

Table 3 :Distribution of Respondents According to Years of Experience

Variable classes	Frequency	Percentage
From 1 to 5 years	8	%6.06
From 6 to 10 years	32	%24.24
From 11 to 15 years	40	%30.30
16years and above	52	%39.39
Total	132	%100

Source: Prepared by researchers based on the results of statistical analysis

3.1.4: Distribution of Respondents According to the Respondents' Knowledge of Cyber Security

Based on Table (4), which shows the distribution of the individuals surveyed according to their knowledge and knowledge of Cyber Security, which represents a topic related to the tagged research, which is one of its axes. Where it turned out that the majority of the respondents were familiar with and have knowledge of the aforementioned subject, and their percentage reached (%54.55) compared to the percentage of the rest within the category of unfamiliar with Cyber Security, where they reached (%45.45).

Table (4): Distribution of Respondents According to the Respondents' Knowledge of Cyber Security

Variable classes	Frequency	Percentage
Yes	72	%54.55

No	60	%45.45
Total	132	%100

Source: Prepared by researchers based on the results of statistical analysis

3.1.5: Description of the Axes (Variables) of the Research: Data related to the variables of the current field study, which includes opinions and answers on questions and paragraphs, were collected through a survey conducted on a sample of research participants. Statistical methods such as frequency distribution, percentages, arithmetic mean, standard deviation and agreement ratios were used. We should point out here that the direction of opinions was determined based on levels of approval, based on the weighted arithmetic mean of questions or statements, using the Likert five-point scale used in the current field study. The scale was divided into five categories, according to the following table:

Table (5): Estimated Balance According to the Likert Pentameter

Response	Weighted average	Length of period	Level
I don't agree completely.	From 1 to 1.79	0.79	Low
I don't agree	From 1.80 to 2.59	0.79	
neutral	From 2.60 to 3.39	0.79	Medium
agree	From 3.40 to 4.20	0.79	High
I completely agree	From 4.21 to 5	0.8	

Source: Prepared by researchers based on the results of statistical analysis

Based on the table above, if the weighted value of the arithmetic mean is between one score and 1.79, the opinions and answers strongly disagree (not completely agree). If it falls into the category of 80.1 to 59.2, the opinions express disagreement with the contents of the statement in question, and so on, In general if the weighted value of the arithmetic or weighted mean of a paragraph or phrase is between one score and 2.59, the degree of agreement is low (disagreement). If it falls in the category of 2.60 to 3.39, it means that opinions are moving towards neutrality or that the degree of agreement is average. Finally, if the weighted value of the arithmetic mean or weighted of opinions is between 3.40 and 5, it means that the degree of approval was high, meaning that the answers were in agreement with what the statement in question meant.

3.1.6: Description of the " Importance of Cyber Security in Protecting Future Accounting Information":

Through Table (6), which represents the descriptive statistics of the paragraphs of the axis "The importance of Cyber Security in protecting

future accounting information", where it was represented by (7) paragraphs. Shows the following:

1. For the axis as a whole, it tends to agree, by (%77.06) compared to (%1.30) of those who do not agree on the aforementioned axis, and it also turned out that the percentage of neutrals on what was included in the axis concerned amounted to (%21.65) In other words, the answers and opinions tend towards approval and at good levels, and the percentage of importance on (the percentage of agreement) as a whole was (%78.61), meaning that opinions are moving towards the importance of Cyber Security in protecting accounting information, according to the opinions of respondents, and this is confirmed by the value of the arithmetic mean (3.93), which was located Within the extent of acceptance, which came from the Likert quintuple scale adopted in the research.

2. In relation to the phrases mentioned separately, it turns out that the statements (Y4) represented by (that future accounting information contributes to increasing the value of the company) then the opinions are more agreed, meaning that the degree of agreement at the said statement was high, based on the value of the arithmetic mean of (4.12) and the percentage of agreement (%82.42). As for the statement (Y5), which is represented by (contributes to reducing the asymmetry of information between the company's management and stakeholders and thus reducing the costs of the agency), the opinions were agreeing, but to a lesser extent, meaning that the opinions and answers were less in agreement compared to the rest of the statements, but the degree of approval is also considered high, based on the value of the arithmetic mean and the percentage of agreement, which is (3.58) and (%71.52) respectively. We conclude that the aforementioned axis statements were a high degree of consensus where the values of the arithmetic means ranged between (4.12) as the highest value and (3.58) as the lowest value and that this range falls within the high degrees of agreement based on Table (5).

3. With regard to the values of the coefficient of variation mentioned in the table below, where its value indicates the homogeneity and divergence of opinions from each other for phrases or paragraphs.

It turns out that the statement (Y1) represented by (future accounting information is information that refers to current plans and future expectations that enable investors and other users to evaluate the future financial performance of the company) has the lowest value of (%14.34) and therefore the opinions and answers when the said statement were homogeneous. While the statement (Y4) represented by (that future accounting information contributes to increasing the value of the company) the answers to the individuals of the research sample were less homogeneous, meaning more distant from each other and had the largest

value of the coefficient of variation of (%18.71) and can not take the opinions of the respondents somewhat because they were less homogeneous any difference in opinions relatively.

Table (6) : Description of the theme "The Importance of Cyber Security in Protecting Future Accounting Information"

Phrases	#	I strongly disagree	I don't agree	neutral	agree	I strongly agree	Arithmetic mean	Standard deviation	Coefficient of variation	Agreement Ratio
		1	2	3	4	5				
Y1	Frequency	0	0	20	88	24	4.03	0.58	%14.34	%80.61
	%	%0.00	%0.00	%15.15	%66.67	%18.18				
Y2	Frequency	0	8	24	88	12	3.79	0.69	%18.15	%75.76
	%	%0.00	%6.06	%18.18	%66.67	%9.09				
Y3	Frequency	0	0	20	84	28	4.06	0.6	%14.81	%81.21
	%	%0.00	%0.00	%15.15	%63.64	%21.21				
Y4	Frequency	0	0	32	52	48	4.12	0.77	%18.71	%82.42
	%	%0.00	%0.00	%24.24	%39.39	%36.36				
Y5	Frequency	0	4	52	72	4	3.58	0.61	%16.95	%71.52
	%	%0.00	%3.03	%39.39	%54.55	%3.03				
Y6	Frequency	0	0	32	88	12	3.85	0.56	%14.51	%76.97
	%	%0.00	%0.00	%24.24	%66.67	%9.09				
Y7	Frequency	0	0	20	80	32	4.09	0.62	%15.22	%81.82
	%	%0.00	%0.00	%15.15	%60.61	%24.24				
Weighted Average	Frequency	0	12	200	552	160	3.93	0.43	%10.95	%78.61
	%	%0.00	%1.30	%21.65	%59.74	%17.32				
		%1.30			%77.06					

Source: Prepared by researchers based on the results of statistical analysis

3.1.7: Description of Axis "Types of Cyber Security":

3.1.7.1: Description of the "Network Security" Dimension : Through Table (7), which represents the descriptive statistics of the paragraphs after "Network Security", where they were represented by (6) paragraphs. It was found that the percentage of neutrals on what was included in the axis concerned amounted to (%13.13) In other words, the answers and opinions are moving towards approval and good levels, and the percentage of agreement for the phrases of the dimension combined of (%77.68) means

that the opinions are moving towards the importance of Network Security in protecting accounting information, according to the opinions of the respondents, and this is confirmed by the value of the arithmetic mean (3.88), which It fell within the range of acceptance, which came from the Likert five-point scale adopted in the research. On the other hand, at the level of individual statements, it turned out that the statement (X1.1), represented by (Network Security affects the protection of future accounting information through the security of protecting information sent by networks), then the opinions are more agreed, meaning that the degree of agreement at the said statement was high, based on the value of the arithmetic mean of (4.06) and the agreement rate (%81.21). As for the statement (X1.6), represented by (Network Security affects the protection of future accounting information by working to support and protect the various communication channels used to access data and information), the opinions were in agreement, but to a lesser extent, meaning that the opinions and answers were less in agreement compared to the rest of the statements, but the degree of approval is also high, based on the value of the arithmetic mean and the percentage of agreement, which is (3.79) and (%75.76), respectively. We conclude that the statements of the aforementioned axis were a high degree of consensus where the values of the arithmetic means ranged between (4.06) as the highest value and (3.79) as the lowest value and that this range falls within the high degrees of agreement based on Table (5).

Table (7): Description of the axis "Network Security"

Phrases	#	I strongly disagree	I don't agree	neutral	agree	I strongly agree	Arithmetic mean	Standard deviation	Coefficient of variation	Agreement Ratio
		1	2	3	4	5				
X1.1	Frequency	0	0	16	92	24	4.06	0.55	%13.51	%81.21
	%	%0.00	%0.00	%12.12	%69.70	%18.18				
X1.2	Frequency	4	4	8	108	8	3.85	0.7	%18.28	%76.97
	%	%3.03	%3.03	%6.06	%81.82	%6.06				
X1.3	Frequency	4	0	24	92	12	3.82	0.72	%18.80	%76.36
	%	%3.03	%0.00	%18.18	%69.70	%9.09				
X1.4	Frequency	0	4	4	116	8	3.97	0.46	%11.61	%79.39
	%	%0.00	%3.03	%3.03	%87.88	%6.06				
X1.5	Frequency	0	4	28	88	12	3.82	0.63	%16.42	%76.36

	%	%0.00	%3.03	%21.21	%66.67	%9.09				
X1.6	Frequency	4	0	24	96	8	3.79	0.69	%18.15	%75.76
	%	%3.03	%0.00	%18.18	%72.73	%6.06				
Weighted Average	Frequency	12	12	104	592	72	3.88	0.36	9.20%	77.68%
	%	%1.52	%1.52	%13.13	%74.75	%9.09				
		%3.03			%83.84					

Source: Prepared by researchers based on the results of statistical analysis

Finally, with regard to the values of the coefficient of variation mentioned in the table below, it was found that the statement (X1.4) represented by (Network Security affects the protection of future accounting information by restricting access to networks to a small number of individuals) has the lowest value of (%11.61) and therefore the opinions and answers when the said statement were homogeneous. While the statement (X1.3) represented by (Network Security affects the protection of future accounting information by setting complex passwords and on more than one stage) the answers to the individuals of the research sample were less homogeneous, meaning more distant from each other and had the largest value of the coefficient of variation of (%18.80) and can not take the opinions of the respondents somewhat because they were less homogeneous any difference in opinions relatively.

3.1.7.2: Description of the "Cloud Security" Dimension : Through Table (8), which represents the descriptive statistics of the paragraphs after "Cloud Security", where they were represented by (6) paragraphs. It was found that the percentage of neutrals on what was included in the axis concerned amounted to (%17.68) In other words, the answers and opinions are moving towards approval and good levels, and the percentage of agreement for the phrases of the dimension combined of (%78.08) means that opinions are moving towards the importance of Cloud Security in protecting accounting information, according to the opinions of respondents, and this is reinforced by the value of the arithmetic mean (3.90), which It fell within the range of acceptance, which came from the Likert five-point scale adopted in the research. On the other hand, at the level of individual statements, it turns out that the two phrases (X2.1 and X2.6), represented by (Network Security affects the protection of future accounting information by ensuring that there is no unauthorized access to the cloud through other networks) and (Network Security affects the protection of future accounting information by ensuring that there is no unauthorized access to the cloud through other networks. Stop unwanted programs that may interfere with The company's network is from other networks in the cloud) where the opinions are more

agreeable, meaning that the degree of agreement at the two statements mentioned was high, based on the value of the arithmetic mean of (4.03) and the agreement rate (%80.61) for each of the two phrases mentioned. As for the two statements (X2.3 and X2.5), represented by (Network Security affects the protection of future accounting information by forcing users to find complex passwords and questions to allow them to access their accounts) and (Network Security affects the protection of future accounting information through technicians sharing external information on the cloud by the company with others), the opinions were in agreement, but to a lesser extent, that is, the opinions and answers were less in agreement compared to the rest of the statements, but the degree of approval It is also considered high, based on the value of the arithmetic mean and the percentage of agreement, which is (3.82) and (%76.36) for each of the two statements. We conclude that the aforementioned axis statements were a high degree of consensus, as the values of the arithmetic mean ranged between (4.03) as the highest value and (3.82) as the lowest value, and that this range falls within the high degrees of agreement, based on Table (5).

Table (8): Description of the "Cloud Security" axis

Phrases	#	I strongly disagree	I don't agree	neutral	agree	I strongly agree	Arithmetic mean	Standard deviation	Coefficient of variation	Agreement Ratio
		1	2	3	4	5				
X2.1	Frequency	4	4	4	92	28	4.03	0.8	%19.83	%80.61
	%	%3.03	%3.03	%3.03	%69.70	%21.21				
X2.2	Frequency	0	0	24	100	8	3.88	0.48	%12.33	%77.58
	%	%0.00	%0.00	%18.18	%75.76	%6.06				
X2.3	Frequency	4	0	20	100	8	3.82	0.67	%17.65	%76.36
	%	%3.03	%0.00	%15.15	%75.76	%6.06				
X2.4	Frequency	0	0	28	96	8	3.85	0.5	%13.02	%76.97
	%	%0.00	%0.00	%21.21	%72.73	%6.06				
X2.5	Frequency	0	0	44	68	20	3.82	0.67	%17.65	%76.36
	%	%0.00	%0.00	%33.33	%51.52	%15.15				
X2.6	Frequ	0	0	20	88	24	4.03	0.58	%14.3	%80.6

	ency								4	1
	%	%0.00	%0.00	%15.15	%66.67	%18.18				
Weighted Average	Frequency	8	4	140	544	96	3.9	0.42	%10.85	%78.08
	%	%1.01	%0.51	%17.68	%68.69	%12.12				
		%1.52			%80.81					

Source: Prepared by researchers based on the results of statistical analysis

Finally, with regard to the values of the coefficient of variation mentioned in the table below, it turns out that the statement (X2.2) represented by (The security of the cloud affects the protection of future accounting information through the customer securing the interfaces correctly for the electronic infrastructure) has the lowest value of (%12.33) and therefore the opinions and answers when the said statement was homogeneous. While the statement (X2.1) represented by (The security of the cloud affects the protection of future accounting information by ensuring that there is no unauthorized access to the cloud through other networks), the answers to the individuals of the research sample were less homogeneous, meaning more distant from each other and had the largest value of the coefficient of variation of (%18.80) and the opinions of the respondents cannot be taken somewhat because they were less homogeneous, i.e. there is a difference in opinions relatively.

3.1.7.3: Description of the "Application Security" Dimension : Through Table (9), which represents the descriptive statistics of the paragraphs after "Application Security", where it was represented by (6) paragraphs. It was found that the percentage of neutrals on what was included in the axis concerned amounted to (%17.68) In other words, the answers and opinions are moving towards approval and good levels, and the percentage of agreement for the phrases of the dimension combined of (%78.99) means that opinions tend towards the importance of Application OF Security in protecting accounting information, according to the opinions of respondents, and this is reinforced by the value of the arithmetic mean (3.95), which It fell within the range of acceptance, which came from the Likert five-point scale adopted in the research. On the other hand, at the level of individual statements, it turned out that the statement (X3.2) represented by (the Security of Applications affects the protection of future accounting information by conducting a test to verify the extent to which applications meet security requirements) then the opinions are more agreeable, meaning that the degree of agreement at the said statement was high, based on the value of the arithmetic mean of (4.09) and the agreement rate (%81.82). As for the statement (X3.1), which is represented by (Application OF Security

affects the protection of future accounting information through the use of security development standards for applications), the opinions were in agreement, but to a lesser extent, meaning that the opinions and answers were less in agreement compared to the rest of the statements, but the degree of approval is also high, based on the value of the arithmetic mean and the percentage of agreement, which is (3.79) and (%75.76). We conclude that the statements of the aforementioned axis were a high degree of consensus where the values of the arithmetic means ranged between (4.09) as the highest value and (3.79) as the lowest value and that this range falls within the high degrees of agreement based on Table (5).

Table (9): Description of the Application OF Security axis

Phrases	#	I strongly disagree	I don't agree	neutral	agree	I strongly agree	Arithmetic mean	Standard deviation	Coefficient of variation	Agreement Ratio
		1	2	3	4	5				
X3.1	Frequency	0	0	36	88	8	3.79	0.54	%14.21	%75.76
	%	%0.00	%0.00	%27.27	%66.67	%6.06				
X3.2	Frequency	0	0	12	96	24	4.09	0.52	%12.60	%81.82
	%	%0.00	%0.00	%9.09	%72.73	%18.18				
X3.3	Frequency	0	0	28	88	16	3.91	0.57	%14.62	%78.18
	%	%0.00	%0.00	%21.21	%66.67	%12.12				
X3.4	Frequency	4	0	24	84	20	3.88	0.77	%19.88	%77.58
	%	3.03%	%0.00	%18.18	%63.64	%15.15				
X3.5	Frequency	0	0	28	76	28	4	0.65	%16.32	%80.00
	%	%0.00	%0.00	%21.21	%57.58	%21.21				
X3.6	Frequency	0	0	12	104	16	4.03	0.46	%11.43 %	%80.61
	%	%0.00	%0.00	%9.09	%78.79	%12.12				
Weighted Average	Frequency	0	0	140	536	112	3.95	0.44	%11.14 %	%78.99
	%	%0.51	%0.00	%17.68	%67.68	%14.14				
		%0.51			%81.82					

Source: Prepared by researchers based on the results of statistical analysis

Finally, with regard to the values of the coefficient of variation mentioned in the table below, it was found that the statement (X3.6) represented by (Application OF Security affects the protection of future accounting information through the existence of Application OF Security policies in the

company) has the lowest value of (%11.43) and therefore the opinions and answers when the said statement was homogeneous. While the statement (X3.4) represented by (the security of the cloud affects the protection of future accounting information through the presence of experts specialized in the Security of Applications with the company) the answers to the individuals of the research sample were less homogeneous, meaning more distant from each other and had the largest value of the coefficient of variation of (%19.88) and can not take the opinions of the respondents somewhat because they were less homogeneous any difference in opinions relatively.

3.2: Testing Research Hypotheses:

to determine the relations between the study variables that illustrated in research framework, it's important to test the research hypotheses which reflect the variables relations. The following section have an explanation about the research hypotheses:

3.2.1: The First Hypothesis

For the purpose of testing the impact relationship of the variable types of Cyber Security in its three dimensions, which include: Network Security, Cloud Security and Application OF Security grouped as an independent variable in the approved variable, represented by the protection of future accounting information and through the results shown in Table (10), where it was found that there is a significant impact of the variable types of Cyber Security in the variable of protection of future accounting information, depending on the value of the level of statistical significance of the model, based on the test (F) of (0.000), which was less than the level of significance The statistical assumed in the study in question of (0.05) and also through the calculated value of the test (F) of (105.199), which was greater than its tabular value of (3.91) at the degrees of freedom (130) and the level of statistical significance assumed of (0.05) In other words, the acceptance of the first hypothesis, which came out of the current study, meaning that there is a statistically significant effect of the types of Cyber Security on the protection of future accounting information.

Through the regression model, we also find that the values of the regression coefficient from the parameters of the regression constant (B0) and the slope (B1) were also statistically significant, based on the level of statistical significance of the two model parameters, where their values were respectively (0.000) for each of the two parameters less than the level of statistical significance assumed in the current study of (0.05), in other words, when there are no types of Cyber Security, the levels of protection of future accounting information are present in a fixed amount of (0.993), as well as when the levels of security types change. By one unit, the levels of

protection of future accounting information change by (0.751) and in the same direction.

Through the coefficient of determination (R2), it was found that the types of Cyber Security explain the changes that occur in the protection of future accounting information by (%34.60), while the remaining percentage (%65.40) is due to other variables that affect the variable of protecting future accounting information that is not included in the model.

Table (10): The Impact of Types of Cyber Security on the Protection of Future Accounting Information

Independent Variable / Dependent Variable	Protection of Future Accounting Information			
	Hard (B0)	Borderline Slope (B1)	F	R2
Types of Cyber Security	0.993	0.751	105.199	%34.60
	T (3.456)	T (10.256)	sig.(0.000)	
	sig.(0.000)	sig.(0.000)		
** High morale when sig≤ (0.01)		F(0.05,1,130)=3.91		

Source: Prepared by researchers based on the results of statistical analysis

3.2.2: Second Hypothesis

For the purpose of testing the impact relationship of Network Security as an independent variable in the approved variable, represented by the protection of future accounting information, and through the results shown in Table (11), where it was found that there is a significant impact of the Network Security variable in the future accounting information protection variable, depending on the value of the level of statistical significance of the model, based on the (F) test of (0.000), which was less than the level of statistical significance assumed in the study concerned of (0.05) and also through the calculated value of the (F) test of (23.062) Which was greater than its tabular value of (3.91) at degrees of freedom (130) and the level of assumed statistical significance of (0.05), in other words, acceptance of the second hypothesis, which came from the current study, meaning that there is a statistically significant impact of Network Security on the protection of future accounting information.

Through the regression model, we also find that the values of the regression coefficient from the parameters of the regression constant (B0) and the slope (B1) were also statistically significant, based on the level of statistical significance of the two model parameters, where their values were respectively (0.000) for each of the two parameters less than the level of statistical significance assumed in the current study of (0.05) In other words, when there is no Network Security, the levels of protection of future accounting information are present by a fixed amount of (2.413), as well as

when Network Security levels change by One unit, the levels of protection of future accounting information change by (0.391) and in the same direction.

Through the coefficient of determination (R2), it was found that Network Security explains the changes that occur in the protection of future accounting information by (%10.50) while the remaining percentage (%89.50) is due to other variables that affect the variable of protection of future accounting information that is not included in the model.

Table (11): The Impact of Network Security on the Protection of Future Accounting Information

Independent Variable / Dependent Variable	Protection of Future Accounting Information			
	Hard	Borderline Slope	F	R^2
	(B0)	(B1)		
Network Security	2.413	0.391	23.062	%10.50
	T (7.599)	T (4.802)	sig.(0.000)	
	sig.(0.000)	sig.(0.000)		
** High morale when sig≤ (0.01)		F(0.05,1,130)=3.91		

Source: Prepared by researchers based on the results of statistical analysis

3.2.3: Third Hypothesis

For the purpose of testing the impact relationship of Cloud Security as an independent variable in the approved variable, represented by the protection of future accounting information, and through the results shown in Table (12), where it was found that there is a significant impact of the Cloud Security variable in the future accounting information protection variable, depending on the value of the level of statistical significance of the model, based on the (F) test of (0.000), which was less than the level of statistical significance assumed in the study concerned of (0.05) and also through the calculated value of the (F) test of (124.619) Which was greater than its tabular value of (3.91) at degrees of freedom (130) and the level of assumed statistical significance of (0.05), in other words, acceptance of the third hypothesis, which came from the current study, meaning that there is a statistically significant effect of Cloud Security on the protection of future accounting information.

Through the regression model, we also find that the values of the regression coefficient from the parameters of the regression constant (B0) and the slope (B1) were also statistically significant, based on the level of statistical significance of the two model parameters, where their values were

respectively (0.000) for each of the two parameters less than the level of statistical significance assumed in the current study of (0.05) In other words, when Cloud Security is absent, the levels of protection of future accounting information are present by a fixed amount of (1.457), as well as when Cloud Security levels change by One unit, the levels of protection of future accounting information change by (0.634) and in the same direction.

Through the coefficient of determination (R2), it was found that Cloud Security explains the changes that occur in the protection of future accounting information by (%38.87), while the remaining percentage (%61.13) is due to other variables that affect the variable of protecting future accounting information that is not included in the model.

Table (12): The Impact of Cloud Security on the Protection of Future Accounting Information

Independent Variable / Dependent Variable	Protection of Future Accounting Information			
	Hard	Borderline slope	F	R^2
	(B0)	(B1)		
Cloud Security	1.457	0.634	124.619	%38.87
	T (6.534)	T (11.163)	sig.(0.000)	
	sig.(0.000)	sig.(0.000)		

** High morale when sig≤ (0.01)
F (0.05,1,130)=3.91

Source: Prepared by researchers based on the results of statistical analysis

3.2.4: Fourth Hypothesis:

In order to test the impact relationship of Application OF Security as an independent variable in the approved variable, represented by the protection of future accounting information, and through the results shown in Table (13), where it was found that there is a significant impact of the Application OF Security variable in the future accounting information protection variable, depending on the value of the level of statistical significance of the model, based on the (F) test of (0.000), which was less than the level of statistical significance assumed in the study in question, which amounted to (0.05) and also through the calculated value of the (F) test of (65.991), which was greater than its tabular value of (3.91) at degrees of freedom (130) and the level of assumed statistical significance of (0.05), in other words, the acceptance of the fourth hypothesis, which came from the current study, meaning that there is a statistically significant impact of Application OF Security on the protection of future accounting information.

Through the regression model, we also find that the values of the regression coefficient from the parameters of the regression constant (B0) and slope

(B1) were also statistically significant, based on the level of statistical significance of the two model parameters, where their values were respectively (0.000) for each of the two parameters less than the level of statistical significance assumed in the current study of (0.05) In other words, when there is no Security of Applications, the levels of protection of future accounting information are present by a fixed amount of (1.992), as well as when the levels of Application OF Security change by One unit, the levels of protection of future accounting information change by (0.491) and in the same direction.

Through the coefficient of determination (R^2), it was found that the Security of Applications explains the changes that occur in the protection of future accounting information by (%25.19), while the remaining percentage (%74.81) is due to other variables that affect the variable of protection of future accounting information that is not included in the model.

Table (13): The Impact of Application OF Security on the Protection of Future Accounting Information

Independent Variable / Dependent variable	Protection of Future Accounting Information			
	Hard	Borderline Slope	F	R^2
	(B0)	(B1)		
Cloud Security	1.992	0.491	65.991	%25.19
	T (8.292)	T (8.123)	sig.(0.000)	
	sig.(0.000)	sig.(0.000)		

** High morale when sig≤ (0.01) F (0.05,1,130)=3.91

Source: Prepared by researchers based on the results of statistical analysis

4.Conclusions and Recommendations

4.1: Conclusions:

This study concerned on the impact of diversity in Cyber Security on protecting the future accounting information. It includes 3 independent variables (Network Security, Cloud Security and Application Security) and one dependent which is (future accounting information Protection).

The cyber-attacks focus on obtaining certain economic benefits such as espionage, financial attacks, card fraud, information theft, phishing, network attacks, intellectual property theft, extortion and others.

In order to address cyber-attack, cyber security emerged with the aim of discovering gaps in the system and working to fix them as soon as they are discovered, through which individuals, companies and systems are protected from cases of digital penetration, unauthorized access or serious security threats, which may affect the privacy of data and information, especially sensitive ones.

In this regard, the result from current study showed that Effective Cyber Security is important in reducing the risk of unauthorized use of related systems, networks and technologies and the ability to resist intentional and unintentional threats. In addition, the results confirmed that tools diversity (Network Security, Cloud Security and Application Security) in Cyber Security help companies to protect future accounting information as resources that help target investors to have a trusted information for decisions making.

Based on above discussion, the study have an important contributions, the first contribution was empirically determining the suitability of various variables. The second contribution was the instrument for collecting data, which is done by using a created questionnaire for this study.

4.2: Recommendations

By reviewing the results of the research, the researchers recommend the following:

1. Companies protect their future accounting information by setting complex passwords, not making company communications available to any third parties without a private encryption key, and conducting a test to verify the extent to which applications meet security requirements.
2. The competent academic authorities represented by universities and institutes operating in the Kurdistan Region add new topics within their curricula, including Cyber Security technology techniques and information security, in order to graduate new competencies aware of this technology and benefit from it in the field of accounting
3. Companies open courses for their employees on how to protect future accounting information, due to the fact that many parties try to penetrate the security system for the purpose of stealing information.

References

1.10.Heroux, Sylvie and Fortin, Anne, 2020, Cyber Security Disclosure by the Companies on the S&P/TSX 60 Index, Accounting Perspectives Journal, Vol. 19, No.2.

2.Alhamdany, Saba Noori(2024), The Effects of Strategic Alertness on the Perceived Quality of working life An analytical study of Fallujah University Staff, Journal of Business Economics for Applied Research, Vol. (6), No. (1), Part (2).

3.Alkhatib, Khalid, 2017, The Determinants of Forward-Looking Information Disclosure, Journal of Management and Accounting Studies, Vol. 5 No. 03.

4.Al-Zubaidi, Zuhair Khudair Abbas and Al-Tamimi, Zafar Abed Matar, 2022, Iraq Cyber Security.. Opportunities and Challenges, Wasit Journal for Humanities and Social Sciences, Vol. 18, No. 51.

5.Arora, Akshay and Khanna, Abhirup and Rastogi, Anmol and Agarwal, Amit, 2017, Cloud Security Ecosystem for Data Security and Privacy, 7th International Conference on Cloud Computing, Data Science & Engineering – Confluence.

6.Asiri, Mohammed, 2021, Three Essays in Investment Efficiency, Accounting Reporting Complexity, and Cyber Security Breaches: Evidence from Corporate Tax Avoidance, PhD thesis, School of Accounting, Curtin University.

7.Badawy, Hebatallah Abd El Salam, 2021, The Impact of Assurance Quality and Level on Cyber Security Risk Management Program on Non Professional Egyptian Investors' Decisions: An Experimental Study, Alexandria Journal of Accounting Research, Vol. 5.

8.Ehioghiren, Efe Efosa and Ojeaga, Joseph Oseikhuemhen and Eneh, Onyinye, 2021, Cyber security : the perspective of accounting professionals in Nigeria, Accounting & Taxation Review, Vol. 5, No. 2.

9.El-Deeb, Mohamed Samy and Elsharkawy, Lamis Mustafa, 2019, The Impact of Board Characteristics on the Disclosure of the Forward Looking Information Evidence from the Egyptian Stock Market, Alexandria Journal of Accounting Research,Vol. 3, No. 3.

10. Gao, Lei and Calderon, Thomas G. Thomas G.ad Tang, Fengchun, 2020, Public companies' Cyber Security risk disclosures, International Journal of Accounting Information Systems, Volume 38.

11. Haapamäki, Elina and Sihvonen, Jukka, 2019, Cyber Security in accounting research, Managerial Auditing Journal, Vol. 34 No. 7.

12. Horne, Craig A. and Ahmad, Atif and Maynard, Sean B., 2016, A Theory on Information Security, Australasian Conference on Information Systems, 6 December 2016, Wollongong, Australia.

13. Hussein, Ebtisam Nafel, 2012, The Impact of the Auditor's Assertive Role through the Audit of Integrated Reports on the Quality of Future Disclosure of Additional Information, Scientific Journal of Business and Environmental Studies, Volume XII, Issue II.

14. Hussein, Mahmoud Mohamed Abdel Rahim, 2020, Analysis of the relationship between optional accounting disclosure of future information in annual reports and the value of the company, Journal of Accounting Studies and Research, second issue.

15. Jain, Ankit Kumar and Sahoo, Somya Ranjan and Kaubiyal, Jyoti, 2021, Online social networks security and privacy: comprehensive review and analysis, Complex & Intelligent Systems, Vol.7.

16. Kaawa, Abeer Ahmed Ali, 2020, Cyber Security Policies to Promote Digital Transformation in Egyptian Universities: A Proposed Vision in the Light of Global Experiences, Journal of Educational and Social Studies, Vol. 26, No. 6.3.

17. Khadeer, Jarjees Mustafa and Mustafa, Bahar Khaled and Mohammed, Nakhshin Jamal, 2022, The Possibility of Applying International Standard on Auditing 3400 to Test Future Financial Information: An Exploratory Study of the Opinions of a Sample of Auditors and Chartered Accountants in the City of Erbil, Iraqi University Journal, Part 2, Issue 53.

18. Khankahdani, Mahboubeh Fotouhi and Taftiyan, Akram and Ardakani, Mehdi Nazmi, 2021, Ranking of indicators of forward-looking information disclosure by the fuzzy analytical hierarchy process, International Journal of Finance and Managerial Accounting, Vol.6, No.21.

19. Kılıç, Merve and Kuzey, Cemil, 2018, Determinants of forward-looking disclosures in integrated reporting, Managerial Auditing Journal, Vol. 33, No. 1.

20. Mansour, Amna Mohammed, 2021, The impact of Cyber Security on internal control and its reflection on the economic unit - an exploratory study of the opinions of a sample of auditors and accountants in the Ministry of Higher Education and Scientific Research, Journal of Administration and Economics, Issue 127.

21. Metwally, Mustafa Zaki Hussein and Gharib, Hussein Abdel-Aal Salem, 2022, Measuring the Impact of Cyber Security Risk Disclosure on External Audit Fees: An Applied Study, Journal of Accounting Thought, Issue 4.

22. Mohsin, Hayder Jerri (2022), The role of banking control tools and their impact on the performance of the work of commercial banks: An exploratory study in a sample of employees of commercial banks in Basra Governorate, Journal of Business Economics for Applied Research, Vol. (5), No. (3).

23. Olson, Stevan K., 2011, Teaching Prospective Financial Statements: A Compilation Project, Journal of Business & Leadership, Volume 7.

24. Rajab, Nashwa Shaker Ali, 2016, Determinants of the Quality of Non-Financial Disclosure of Future Information on the Websites of Companies Included in the EGX30 Index, Journal of Accounting Thought, Volume 20, Issue 4.

25. Rosati, Pierangelo and Gogolin, Fabian and Lynn, Theo, 2020, Cyber-Security Incidents and Audit Quality, European Accounting Review, Volume 31, Issue 3.

26. Sabsabi, Mustafa Youssef, 2021, The Role of Future Financial Information for Companies in Decision-Making: A Field Study on a Number of Private Sector Companies, Master's Thesis, Faculty of Economics, University of Aleppo.

27. Zadorozhnyi, Zenovii Mykhaylo and Muravskyi, Volodymyr and Shevchuk, Innovative accounting methodology of ensuring the interaction of economic and Cyber Security of enterprises, Marketing and Management of Innovations, Issue 4.

Questionnaire form

Gentlemen

Best regards.....

We place in your kind hands the questionnaire form for the research titled (The impact of types of cybersecurity on the protection of future accounting information, an analytical study of the opinions of a sample of professionals and academics in the city of Erbil), hoping to answer its questions with all objectivity and impartiality in order to obtain results that will enrich the research and achieve its goals.

We are grateful for your cooperation in serving the scientific process

note: Please put a mark (√) in the box that represents your answer, and if you have any comments or opinions, they can be added in the last field of the questionnaire.

Please note that this information is used for scientific research purposes only.

Researchers

section One. Personal data:

Job qualification: A. Academic ( ) B. Professional ( ).

Academic qualification: A. PhD ( ) b. Master ( ) c. Bachelor's degree ( ).

Number of years of experience: A. From 1 to 5 years ( ) b. From 6 to 10 years ( ) c. From 11 to 15 years ( ) D. 16 years and above ( ).

Do you have knowledge of the subject of Cyber Security: A. Yes (1) No (2)

Second section. Procedural definitions

Cyber Security: It is a matrix of organizational, technical and procedural tools and practices aimed at protecting computers, networks and the data inside them from penetration, damage, change or disruption of access to information or services.

Future Accounting Information: It is Information related to future plans and forecasts that can be used and benefited by shareholders, creditors, investors, and others.

Section Three. Measuring research variables:

First: The Importance of Cyber Security in Protecting Future Accounting Information.						
No.	**Paragraphs**	**Strongly Agree**	**I Agree**	**Neutral**	**I don"t Agree**	**I Strongly Disagree**
1.	Future Accounting Information is Information that refers to current plans and future projections that enable investors and other users to evaluate the future financial performance of a company.					
2.	Protecting Future Accounting information increases companies' ability to access financial markets.					
3.	Protecting Future Accounting Information will contribute to helping investors better anticipate future profits in addition to improving their ability to evaluate future cash flows.					
4.	Future Accounting Information contributes to increasing the value of the company.					
5.	It contributes to reducing information asymmetry between company management and stakeholders and thus reducing agency costs.					
6.	It helps the company attract more investments and enhance its reputation in the market, thus increasing its ability to compete in the future.					

7.	Future Accounting Information enhances the confidence of financial analysts in the management of the company's affairs.
Second: Network security (one of the types of Cyber Security) affects the protection of Future Accounting Information through:	
8.	Security protection of information sent by networks.
9.	Providing maximum protection for information in networks in order to avoid risks that may be inflicted on them.
10.	Set complex passwords and on more than one stage.
11.	Restrict access to networks to a small number of individuals
12.	Restricting the granting of permission to access the network to one person
13.	Work to support and protect the various communication channels used in order to access data and information.
Third: Cloud Security (one of the types of Cyber Security) affects the protection of future accounting information through:	
14.	Ensure that there is no unauthorized access to the cloud through other networks
15.	The customer secures the interfaces correctly for the electronic infrastructure
16.	Forcing users to find complex passwords and questions to allow them to access their accounts
17.	Increase the company's access to information stored in the cloud
18	Technicians share external information on the cloud by the company with others
19	Stop unwanted software that may interfere with the corporate network from other networks in the cloud
Fourth: Application Security (one of the types of Cyber Security) affects the protection of future accounting information through:	
20.	Use security development standards for applications.
21.	Conduct a test to verify the extent to which applications meet security requirements.
22.	Conduct a review of settings, immunization and update packages before launching any application.
23.	The presence of experts specialized in application security at the company.
24.	Filling security gaps in application security by the company
25.	The existence of policies related to application security in the company.