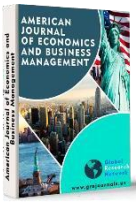

American Journal of Economics and Business Management

Vol. 8 Issue 7 | **pp.** 3585-3611 | **ISSN:** 2576-5973

Available online @ https://www.globalresearchnetwork.us/index.php/ajebm

Article

The Impact of Cybersecurity on Improving The Quality of Accounting Information

Mohammed Sadeq Jappar[1], Ali Kareem Khudhair Abuzabiba[2], Alaa Abdulzahra Obaid[3]

1. University of Kufa, Iraq.
2. University of Kufa, Iraq.
3. University of Kufa, Iraq.

* Correspondence: alik.abuzabiba@uokufa.edu.iq

Abstract: The research aims to test the impact of cybersecurity on the quality of accounting information. To achieve the desired goal, the impact of cybersecurity on the quality of accounting information was measured during the design of the (questionnaire). The target was the banks listed in the Iraqi Stock Exchange. (180) questionnaires were distributed, of which (165) were retrieved, while (123) questionnaires were valid for statistical analysis. The researcher used the five-point Likert scale, as many statistical methods were relied upon to analyze the data and verify the research hypotheses. In addition to achieving one of the research objectives, the quality of accounting information was measured through the price model by applying it to the same sample of banks to which the questionnaire form was distributed for the years (2013-2022). A set of conclusions were reached, the most important of which was that there is an impact of cybersecurity on the quality of accounting information. It revealed statistically significant effects in the predictive value, confirmatory value and relative importance. This confirms the interconnected nature of the dimensions of cybersecurity and the quality of accounting information. The researcher recommended A set of recommendations, the most important of which was the necessity of paying attention to cybersecurity and accounting information technology governance due to their impact on maximizing economic unity and protecting accounting information from cyber attacks, thus maintaining the continuity of the economic unit.

Keywords: Cybersecurity, Accounting Information, Quality, Cyber Attacks, Economic Unit

Citation: Jappar, M. S, Abuzabiba, A. K. K & Obaid, A. A. The Impact of Cybersecurity on Improving The Quality of Accounting Information American Journal of Economics and Business Management 2025, 8(7), 3585-3611

Received: 08th Apr 2025
Revised: 15th May 2025
Accepted: 28th June 2025
Published: 24th July 2025

1. Introduction

Cybersecurity is one of the basic pillars that is gaining increasing importance in light of the rapid technological developments and environmental changes facing economic units. In the age of digitization, accounting information has become one of the most important assets that institutions rely on to make strategic and financial decisions, which makes protecting it from cyber threats of utmost importance [1], [2], [3]. Hence, the need to enhance cybersecurity has emerged to ensure the quality of accounting information, which is a key measure of its reliability and ability to influence the decision-making process.

This study addresses the relationship between cybersecurity and the quality of accounting information, where cybersecurity is defined as the technical, legal and regulatory framework that aims to protect information and digital assets from cyber attacks, while the quality of accounting information refers to its suitability and reliability in serving decision-making purposes [4]. The importance of this study lies in shedding light on how the application of cybersecurity practices affects improving the quality of

accounting information, which contributes to enhancing user confidence and making more effective decisions [5]. In this context, cybersecurity is a crucial element in ensuring the integrity of accounting information and protecting it from breaches and threats that may affect its accuracy and reliability. The quality of accounting information is considered a key indicator of the success of these efforts, as it reflects the ability of information to influence decisions and provide accurate predictions about future events. To achieve the research objectives, the study was organized into four main chapters [6], [7]. The first chapter deals with the research methodology and previous studies, where the theoretical and practical framework of the study is presented. While the second chapter focuses on the theoretical aspect, addressing the concepts of cybersecurity and the quality of accounting information, in addition to the relationship between them [8]. The third chapter deals with the practical aspect by measuring the impact of cybersecurity on the quality of accounting information in the research sample banks, with an analysis of the questionnaire results and testing of hypotheses. Finally, the fourth chapter presents the conclusions and recommendations drawn from the study. This study aims to highlight the vital role of cybersecurity in enhancing the quality of accounting information, which contributes to achieving the goals of economic units and ensuring their sustainability in an environment full of technological and security challenges [9].

2. Materials and Methods

1.2 Research Problem

Most banks listed on the Iraq Stock Exchange suffer from weakness and deficiency in the quality of accounting information, due to the low level of transparency in the financial statements, which negatively affects the degree of reliability and appropriateness of this information. To overcome this problem, the role of cybersecurity emerges as a pivotal factor in enhancing the quality of accounting information by ensuring data protection and increasing its reliability. Therefore, the research problem can be formulated with the following questions:

First: To what extent does cybersecurity affect improving the predictive value of accounting information in Iraqi banks?

Second: To what extent does cybersecurity affect enhancing the confirmatory value of accounting information in Iraqi banks?

Third: To what extent does cybersecurity affect increasing the relative importance of accounting information in Iraqi banks?

2.2 Research Objective

The research seeks to achieve several objectives, which are referred to in the following:

1 .Clarifying the concept of cybersecurity and its dimensions, with a focus on its role in protecting data and enhancing the reliability of accounting information.

2 .Highlight the importance of cybersecurity in ensuring the integrity and safety of accounting information, and its role in enhancing transparency and confidence in financial statements.

3 .Explain the concept and importance of the quality of accounting information, focusing on its dimensions such as relevance, reliability, and confirmatory and predictive value.

4 .Test the impact of cybersecurity in improving the quality of accounting information, by analyzing its role in enhancing relevance and reliability.

5 .Measure the impact of cybersecurity in enhancing the quality of accounting information, focusing on how it improves the predictive and confirmatory value of information.

6 .Analyze the relationship between cybersecurity and the quality of accounting information, with the possibility of referring to the role of IT governance as a supporting factor for cybersecurity in specific cases.

3.2 Importance of the Research

The importance of this research is highlighted in addressing the topic of cybersecurity and its impact on improving the quality of accounting information, as this research

distinguishes - to the best of the researcher's knowledge - in studying the impact of cybersecurity on the quality of accounting information in an integrated manner, with reference to the role of IT governance as a supporting factor in enhancing the effectiveness of cybersecurity.

This research comes at a time when the world is witnessing an increase in the importance of cybersecurity, as many economic units seek to apply its principles and rules as one of the most important areas of technological development at the present time. Interest in cybersecurity helps in providing a safe and transparent work environment, which enhances the credibility of accounting information and raises investor confidence.

In addition, enhancing cybersecurity contributes positively to attracting more internal and external investments, as it is a pivotal factor in ensuring data integrity and protecting information from hacking and electronic threats. To achieve high quality accounting information, effective cybersecurity systems must be available, supported by strong IT governance to ensure the efficiency and effectiveness of these systems.

4.2 Research Hypothesis

The research was based on a main hypothesis: "There is a statistically significant impact of cybersecurity in its dimensions on improving the quality of accounting information in its dimensions".

5.2 Data Collection Methods

The descriptive approach was followed in this research by reviewing the literature represented by studies, research, theses, and university dissertations related to the research topic.

Chapter One

Theoretical Framework

1 .Cybersecurity - Conceptual Introduction

Cybersecurity is an important issue in the modern world as the world becomes more dependent on technology; economic units rely on computer systems and the Internet to keep their jobs and data safe. However, these systems are vulnerable to cyber attacks that can have significant negative effects, as well as cyber attacks can lead to the theft of sensitive data, such as credit card numbers and bank account information [10], [11]. It can also disrupt systems and networks, resulting in significant financial losses in some cases, cyber attacks can damage or disable infrastructure, cybersecurity is one of the priorities of the economic unit. Economic units and individuals should take measures to improve network security, prevent network attacks and prevent losses, as they must have a plan to protect against cyber attacks, and they must be aware of the risks they face [12]. In this section, the concept of cybersecurity and its related concepts will be addressed, and its importance in protecting data and systems. In addition, the classification of cyber threats and the reasons for committing cyber crimes will also be discussed, along with the characteristics of security and the requirements for achieving it. The areas of use of cyber security, its dimensions and threat patterns were also highlighted, with a focus on the obstacles facing the achievement of security[13].

2 .Types of Cypher Security Concepts

The concept of cyber security includes many concepts related to protecting users from cyber risks and victims of violations. Below are some of them based on what was mentioned in many studies that addressed these concepts:

a. Cyberbullying: The meaning of this is the use of communications technology for harmful purposes such as harassment and threats of blackmail. The phenomenon of cyberbullying has spread. With the spread of mobile devices and smartphones, cyber risks have become great. • Cyber Defamation: This is done by broadcasting ideas and news that may cause moral harm to a specific person or entity, with the aim of carrying out such an attack, as the method of attack varies; to the personal website (victim) is distorted and then changing its content, or creating another new website, or publishing inaccurate news and information about that person, and defamation is not limited to individuals, but may extend to educational and political systems as well as religions, by creating or sites that challenge religious beliefs, or

broadcasting fabricated and fabricated news and scandals about them[14],[15].

b. Cyber Fraud: It is a form of deception of the victim. Cyber fraud takes several methods such as deceiving the victim, that there is a fake material, and the perpetrator adopts a fake name and identity, etc., which enables him to arrest the victim, by communicating with the victim through the Internet, or the perpetrator can process computer data directly and use false data to deceive and defraud the victim.
c. Cyber Phishing: This is a form of cybercrime also known as phishing. Through it, users can obtain their sensitive information such as credit details, personal information, passwords, etc. by using emails that appear to be from real parties or through advertisements spread on certain websites [16], [17], [18].
d. Cyber Deception: Young internet users are often the biggest victims of such risks, as perpetrators trick victims into wanting to form friendships online, which may develop as a result of the relationship between the two parties.

3 .The importance of cybersecurity

The importance of cybersecurity can be found in the following.

a. Protecting all devices from hacking to be a protective shield for information. In addition, it provides a highly secure work environment while working on the Internet.
b. Troubleshooting and resolving system errors[19], [20], [21].
c. Cyber risk management reduces the risk of attack and minimizes financial and operational impact.
d. Protecting system resources from unauthorized access, disclosure and modification.
e. One of the keys to improving cybersecurity is a better understanding of the threats that attackers use to evade cyber defenses.
f. The interaction between adversary capabilities, intentions and targeting activities must be taken into account when determining the nature of the cyber threat facing the economic unit.

The importance of network security is increasing day by day, as in addition to being considered a representative of the government's capabilities in protection, it is also related to many different areas and life activities such as the economy, education, society and humanity. Their interests and individuals. It is also the main supporter of continuous progress in all areas of daily life and achieving the desires of ideal development[22], [23], [24].

4 .The importance of cybersecurity was also identified in the following:

a. Cyberattacks have become more advanced. Attackers use a variety of tactics in more complex network operations. These include ransomware, malware, and social engineering.
b. The price of cybersecurity incidents is rising. Economic units that are subject to cybersecurity breaches may be subject to large fines. Non-financial expenses, such as damage to reputation, must also be considered[25] ,[26].
c. Cybersecurity is important for anyone who uses the Internet, as most cyberattacks are automated and target broad vulnerabilities, not specific economic units or websites.
d. At the board level, cybersecurity is a major concern. Monitoring cybersecurity threats is difficult due to reporting rules and new laws. Boards want assurances from management that the approach Information security research occupies a large and growing niche among the various IT studies, and may even become one of the problems that plague all parties [27], [28], [29], [30].

5 .Cybersecurity Objectives

Economic units around the world seek to implement cybersecurity; and to achieve many goals, and the most important goals of cybersecurity are:

a. Enhancing the protection of operational technology systems and their components at all levels, including the devices, programs, services they provide and the data they contain.
b. Provides the necessary requirements to reduce risks against users and cybercrimes.
c. Aims to create a safe and reliable environment for users by protecting information and electronic systems from digital attacks and threats[31].
d. Aims to protect users and information systems from malware, which can cause serious damage.
e. Emphasizes the importance of reducing sabotage and electronic espionage at the level of economic units, as these attacks can cause damage to the digital infrastructure of economic units.

6 .Elements of Cypher Security

With the development of Internet network technology, economic units, users and individuals have begun to search for ways to develop information systems and networks, and caution should be exercised regarding network security [32], [33], [34], [35]. This requires a technical culture that focuses on researching the risks of cyber attacks, and one of the most prominent elements of cybersecurity that participants call for attention to and developing methods to find appropriate solutions to protect the economic unit or individual.

The elements of cybersecurity are explained as follows:

a. Awareness: Participants should understand the needs of information systems and network security and what they can do to improve security.
b. Responsibility: Participants bear responsibility for the security of information systems and networks according to their respective responsibilities. Participants should periodically review their practices, policies, procedures and processes and assess their suitability to their application environment.
c. Response: This is concerned with attention and timely response in order to prevent, identify and respond to security incidents. They should communicate information about threats and vulnerabilities to each other and establish procedures for cooperating effectively and quickly to prevent, identify and respond to such incidents [36], [37]. This may include information sharing and cross-border cooperation.
d. Ethics: As information systems and networks permeate every corner of modern society, participants are required to take into account the legitimate interests of others and recognize that their actions or inactions may harm other people[38], [39].
e. Democracy: By promoting security in a manner consistent with the values of a democratic society, including the free exchange of ideas and the free flow of information, confidential information and communications, appropriate protection of personal information, and openness and publicity.
f. Risk assessment: All participants should conduct regular risk assessments to identify threats and vulnerabilities broadly enough to cover key internal and external factors, such as applied technologies, physical, human and system factors, and third-party services that affect security, thereby determining acceptable levels of risk, and assisting in the selection of appropriate controls to mitigate the risk of potential harm to information systems and networks, taking into account the nature and importance of the information being protected
g. Design and implementation of security features: The safety of participants should be considered of utmost importance in the planning, design, operation and use of information systems and networks.
h. Security Management: Participants follow a comprehensive approach to security management based on dynamic risk assessments, covering all participants' activities and all aspects of their operations.

i. Revaluation: Participants review and assess the safety of information systems and communications networks and make adjustments to security policies, procedures, practices and measures, taking into account the increasing prevalence of new risks and vulnerabilities [40], [41], [42]

7 .Classification of electronic threats

Cybercriminals can come from inside or outside the economic unit in the face of cyber attacks. Based on this fact, cybercrimes can be divided into two types

•Insider Threat: An attack is carried out from inside by someone who has access to a network or computer system. This is often done by internal employees. The motive of the insider may stem from revenge or greed. Due to his knowledge of the rules and practices of security systems and the structure and strength of information technology, insiders can carry out cyber attacks with little effort. Hackers can also access the network. Therefore, it is easy for an insider to steal important data. Insider attacks usually occur when someone is fired or given a new job in an economic unit that is not specified in the IT standards. This gives the attacker an authentication window. The internal intrusion detection system of the economic unit may be able to stop an insider attack[43] .

•The threat from abroad: External attacks occur when an attacker is hired by someone or an employee from outside the economic unit. Economic units exposed to cyber attacks suffer damage to their reputation and financial loss. The attacker often scans and collects data because he is not a member of the group. Since external threats can be detected by examining these firewall logs, skilled security network administrators monitor them. There is also an intrusion detection system to monitor any threats from the outside.

8 .Cybersecurity features

If cybercrime is carried out according to modern methodologies and methods with a higher technological dimension than traditional crime, to overcome this and keep pace with the pace of technological development, the emergence of cybersecurity is very necessary. Therefore, cybersecurity offers several features, the most prominent of which are.

a. Detection and tracking: Cybersecurity aims to detect cybercrimes, track their impact, and then overcome them.
b. Speed and lack of evidence: The difficulty of proving cybercrimes is evident in the fact that hackers use modern and constantly evolving technological means. Therefore, it is necessary for cybersecurity to adopt high technology that exceeds its skills and expertise.
c. The weakness of security and judicial agencies in dealing with cybercrimes: This is due to the lack of digital expertise among security agencies, all of which enhances the role of cybersecurity in achieving digital security for economic units, and protecting the data and infrastructure of these devices.

Al-Mutairi also adds a set of characteristics that are represented in the following:

1. Cybersecurity is not a one-time course of action, but rather an ongoing process and contains innovative defense mechanisms because it confronts threats to systems, networks, and others.
2. It works to create a secure cyber ecosystem and establish a reliable system.
2. It carries out a preemptive control process with the aim of searching for risks and working to solve them and close the gaps.
3. It works on subsequent defense, which is represented in the rule of returning the situation to what it was.
4. Provides the feature of alerting to the presence of an error or misuse of networks that expose data and information to danger from within the economic unit, as well as covering external risks and monitoring threats.
5. 9 .Requirements for Achieving Cybersecurity

The requirements for achieving cybersecurity are

a. Defining work procedures in the information network: The content that is allowed or not allowed for network information security must be clear and specific.

b. Ensuring the necessary mechanisms for implementing the work policy: To enable clear and accurate implementation of work policies and determine penalties in case of non-compliance.
c. Human resources: The management and operation of information networks must be assigned to qualified, trained and qualified employees to deal with modern technology and no room for tampering with the capabilities of national government agencies is allowed.
d. Updating the original status of network devices: As a precautionary measure, the original status of devices connected to the information network is changed periodically, which helps prevent external hacking.
e. Monitoring: The need to ensure accurate and continuous monitoring and tracking of information activity on the network.

10 .Dimensions of cybersecurity

Cybersecurity affects all social, political, military, economic and legal issues and aims to achieve an integrated security system dedicated to protecting national security from all cyber threats. Therefore, the dimensions of cybersecurity must be clarified, which are as follows:

a. Social dimension: The international information network is an open field for all, and all network operators can benefit from its infrastructure and available services without security risks. Here, the need to feel the ethics of cybersecurity must be recognized. There are currently more than 4 billion (Internet) users worldwide, 2.6 billion of whom use social networking sites, making it the largest concentration of human interaction. It opens the door to the exchange of good ideas and experiences, but in turn, it exposes the morals of society to danger due to the difficulty of monitoring Internet content, and it also exposes identities to external infiltration operations that may pose a threat to social peace in the country, so we must work hard to educate citizens about these risks in order to achieve cybersecurity at the community level,[44].
b. Political dimension: States have the right to protect their institutions and political interests, and shifts in the balance of power, allowing citizens to be key players who can understand the context of political decisions through the vast amount of information they can easily obtain. For example, we mention here the leaking of sensitive documents, which raises major issues, and the role of social media networks in organizing political and electoral propaganda, organizing virtual demonstrations, and creating electronic protests. A recruitment haven for terrorist organizations and many ideological and religious propaganda, this has become a threat to social cohesion [45].
c. Military dimension: The Internet originally emerged in a military environment and has since grown rapidly to move to different scientific and academic circles in another context, in addition to research that serves military capabilities and represents the relative advantage of the army's cybersecurity capabilities through cyber power, through a virtual world that connects military units, facilitating the exchange of information, which has a positive impact on achieving the highest military goals. States use cyberspace for security and military considerations, and many countries have entered cyberspace to achieve economic prosperity, obtain resources of wealth and power, and achieve political dominance.
d. The economic dimension: Cybersecurity is closely linked to the economy. There is a clear relationship between the knowledge economy and the expansion of the use of information and communication technologies and the value represented by data and information that are traded, stored and used at all levels [46]. Information and communication technologies can also contribute to economic development. Many countries, whose development has benefited from the access provided by international economic units and

major economic units, seek to manage production costs in the best possible way. However, this bright reality raises questions, whether it is the protection of service providers, jobs, or Internet consumers [47], [48].

e. The legal dimension: Individual, institutional and governmental activities in cyberspace arrange legal outcomes and obligations that require attention in order to find rules to resolve disputes that may arise. Therefore, it is necessary to consider some of the transformations accompanying the emergence of the information society. In addition to the basic rights and human freedoms recognized in the Constitution and the International Charter, other rights have been added, such as the right to access global information networks [49], [50]. Abu Hussein also adds that those responsible for government capacity and policies have a clear link between security and economic growth. Cybersecurity ensures that the public enjoys the services provided by ICT and ensures the public's demand for ICT, which in practice translates into the development of a sound economy [51].

11 .Challenges of implementing cybersecurity

1. There are no statistics and information about individual victims of cybercrimes due to lack of timely reporting or never reporting, due, on the one hand, to lack of awareness and understanding of the subject, and on the other hand, to lack of trust in the relevant security agencies, or even lack of awareness of their existence at the national level.
2. The lack of a clear definition of cybercrime perpetrators and their victims makes it impossible to determine the characteristics of cybercrimes [52].
3. Cyberspace: With all the developments witnessed by the digital world, it constitutes a dynamic and constantly changing digital environment, in which it is difficult to understand the phenomenon of cybercrime.

12 .Quality of accounting information - a conceptual approach

Accounting information is one of the basic components of an integrated decision-making system, as it is considered one of the most important tools that management relies on in the process of making strategic and financial decisions. In fact, one of the main reasons for the emergence of accounting and its continuous development is its ability to provide accurate and high-quality information that contributes to supporting the decision-making process. Accounting information has several characteristics that make it useful and effective, such as its ability to predict future income and provide valuable insights into financial performanc In this context, the quality of accounting information is a pivotal element in enhancing the effectiveness of financial decisions, as it reflects its reliability and suitability to the needs of its users. As a result, this section will study the concept of accounting information quality, focusing on the most important models and frameworks that can be used to measure this quality, including the relevance of information and its ability to influence the decision-making process.[53]

13 .The importance of the quality of accounting information

There are many points of view that have focused on studying the quality of accounting information, and we will discuss them in detail according to the opinions of the following authors:

These opinions are represented in the following points:

First - The importance of the quality of accounting information for the growth of the stock market: The quality of accounting information is of paramount importance for the growth and development of the stock market. When the financial statements are of high quality and appropriate, they reflect the efficiency of the accounting standards and practices followed, and they also show the maturity of the local financial market and its ability to provide reliable information to investors.

Second - The role of information quality in assessing market efficiency: Studying the quality of accounting information helps in assessing the efficiency of the financial market. In markets with information efficiency, securities prices depend largely on the available information, which is carefully analyzed to determine the effectiveness of the market and its ability to accurately reflect financial data.

Third - The importance of information quality for regulators and accounting professionals: The quality of accounting information is of great value to those responsible for regulating the accounting profession, as it helps them assess the reliability of financial statements, especially in difficult economic conditions. It also contributes to enhancing confidence in the accounting practices followed.

Fourth - The impact of difficult conditions on the quality of accounting information: Economic crises, such as the global financial crisis, demonstrate the importance of the quality of accounting information. In such circumstances, it is possible to understand the extent to which these crises negatively affect the quality of accounting information and the confidence of economic units in the financial statements that are prepared.

Fifth - The benefit of information quality for investors and market users: The importance of the quality of accounting information is not limited to investors only, but extends to all market users. Investors rely on accounting information to make sound investment decisions, while other market participants, such as creditors, customers and governments, benefit from it to make effective economic decisions.

Sixth: The importance of information quality for investors and decision-making: The quality of accounting information is of great importance to investors, as they are the main users of financial statements. They rely on this information to evaluate financial performance, predict future returns, and estimate the cost of capital. In addition, the quality of information contributes to understanding its impact on stock prices and returns, making it a vital tool for making informed investment decisions. This quality also benefits other parties, such as creditors, governments, and academics, who rely on accounting information in making their economic decisions.

14 .Reasons for the increasing importance of the relevance of the value of accounting information:

The main reasons for the increasing importance of the relevance of the value of accounting information can be described as follows.

a. It is important in expanding people's awareness of the importance and reliability of accounting numbers, which are closely related to stock prices. Accounting reflects accounting numbers that are relevant to investors and important in evaluating the economic unit.
b. The increase in the size of economic units and the impact of technological industries on the book value and profit value of assets, respectively, due to the importance of intangible assets for these economic units. Accounting information is also less important to investors if they focus on the economic unit.
c. The size of reported losses has increased over time for economic units, and this clearly affects the book value of the share and the profit value, and the increase in the size of losses over time may lead to a decrease in profits[54].
d. The importance of financial statements for both economic units and the public in general lies in communicating with shareholders. The use of accounting figures to increase analysts' expected income is one example of applying value studies to accurately forecast revenues.
e. Shareholders' desire to meet their interests, through which they can address analysts' bias in forecasting, which enhances the accuracy of current estimates, and the definition of fundamental analysis is to identify ways to use accounting information to produce quality earnings estimates.

15 .Characteristics of the quality of accounting information

The study of Al-Sayed referred to the characteristics of the quality of accounting information, which were summarized in the following points

First - The relationship of accounting information to the evaluation of economic units: The idea of the quality of accounting information is represented in the extent of its ability to reflect the true values of economic units, as it is verified how the accounting numbers resulting from accounting measurements are related to the information that investors rely on to evaluate the performance of economic units.

Second - The role of standard-setting bodies in enhancing the quality of information: The quality of accounting information is closely related to accounting standard-setting bodies and institutions, as these bodies provide a standard framework that ensures that accounting information is of high quality and appropriate to the needs of users, including professionals and academics.

Third - Using accounting principles to enhance quality: The application of accounting principles developed by the Financial Accounting Standards Board (FASB) aims to enhance the quality of accounting information, as the appropriateness and objectivity of accounting figures are evaluated according to these standards, which increases their reliability and usefulness.

Fourth - The relationship between information quality and conservative accounting practices: The quality of accounting information is consistent with the study of conservative accounting practices, as these practices show the nature of accounting work and their impact on the quality of information. This highlights the importance of studying the quality of information in understanding and analyzing conservative accounting practices.

Fifth - The ability of accounting information to explain changes in markets: The quality of accounting information is not limited to its use in evaluating economic units only, but also includes its ability to explain changes in stock prices over time or between different economic units. This reflects the effectiveness of accounting information in explaining market fluctuations and supporting investment decisions retrospectively.

16 .Quality of accounting information and relevance of the value of accounting information

First: Qualitative characteristics of accounting information: In order for financial information to be useful, it must possess the basic qualities of relevance and honest representation. Both are crucial and important, as information is of little value if it is not appropriate. Even if the information is appropriate, it will not be equally useful if it does not honestly represent the economic phenomenon it aims to represent. There are two basic features that must be provided in accounting information, and their absence negates the intended benefits:

1 .Relevance: "The relevance of accounting information depends on its ability to influence decision-making, as a sound decision cannot be reached without relying on appropriate information. Accordingly, decision-makers must be provided with this information upon completion of the preparation of that information, the value of which appears when making the decision.

"Relevance means that accounting information is able to influence decision-makers. The appropriate information helps its users to make predictions about the outcome of past, current and future events, the predictive value of information, and the appropriate information is that which helps its users to support or correct their future expectations, i.e. this information has the ability to provide feedback, and therefore the appropriate accounting information must be characterized by predictive value and feedback"

In order for the information to be appropriate, it must have the following:

a. Predictive value: Relevant information often provides feedback and predictive capabilities, as knowledge of past activities and impacts improves decision makers' ability to predict the outcomes of similar future actions. While added that information has predictive value if it can be used as an input to a process by which users of financial reports form their own expectations about future outcomes. Information that is characterized by its ability to support decision makers in increasing the likelihood of making accurate predictions of future events is described as having predictive value. For example, if the amount of net profit measured on a present value basis rather than a historical cost basis more accurately predicts the expected future cash flows of an economic unit, it can be said that the present value basis is more appropriate than information prepared on a historical cost basis because of its high relative predictive value.
b. Confirmatory value: It was defined by (Al-Qasaimeh) as one of the benefits of accounting information. If decision makers can verify the validity of their past

expectations, they can evaluate the results of the decisions based on those expectations, as accounting information has a confirmatory value if feedback is provided.

c. Materiality: This rule determines the importance of accounting information to its users, and indicates the need to classify and organize information in financial reports in order to make decisions according to their relative importance. The condition of paying attention to the importance and content of accounting information was also included, instead of overemphasizing the form or image. In the end, the availability of these features in accounting information has a direct and significant impact on the various administrative functions, because most of these functions depend on accounting information. These features are also integrated in an integrated manner, as they provide an objective means of comparison that ensures that the gain is derived from financial reports, especially for internal purposes.

Faithful Representation: For information to be useful in preparing financial reports, the representation of economic phenomena must be a true representation. Faithful representation is achieved when the depiction of the phenomenon is complete, neutral, and free from material error. Information that faithfully represents an economic or other phenomenon depicts the essence of the underlying transaction, event, activity, or other circumstance, which is not necessarily always the same as its legal form. In practice, it may not be possible to know or confirm whether the information provided is complete, neutral, and free from material errors. However, the information should be complete, neutral, and free from material errors as much as possible.

a. Neutrality: The information contained in the financial statements must be objective and free from bias. Financial information is considered neutral unless the method of selecting or presenting the information has a direct impact on the decision-making process or judgment for a specific purpose.
b. Completeness: To ensure the accuracy of information, financial statements should be complete within the relevant relative importance limits, and any discrepancy in information will lead to a misunderstanding or incorrect conclusion, which cannot be relied upon. As (Malouh) adds, in order to be credible, the information contained in the financial statements must be complete. This means that omissions in information may lead to error or ambiguity, both of which are dishonest and inappropriate.
c. Free From Error: It means that there are no errors or omissions in describing the event, and the method of producing the reported information has been used without errors. In this context, it is important to realize that freedom from error does not necessarily mean complete accuracy in every aspect. For example, an accurate estimate of a price or value that cannot be observed cannot be inferred. However, the representation of this number can be accurate if the description is detailed and accurate, the nature and limitations of the estimation process are explained, and no errors are made in choosing or applying the appropriate process for forming estimates.

Second: Secondary characteristics of accounting information: These characteristics must be available in accounting information so that the information is more useful, and their absence does not mean that the information is useless, as the secondary characteristics include the following:

1. Comparability: It is the ability to compare the financial reports of economic units by users. It is a secondary qualitative characteristic that allows users to distinguish and understand the differences and similarities between the elements. As (Al-Awam) adds, the policy allows comparing financial statements from one period with financial statements from another period due to the difference in accounting policies and rules used in preparing these statements.
2. Verifiability: It means that the specific results achieved by a specific person can be achieved by another person, using the same measurement and disclosure methods used.

3. Timeliness: It means providing information at the right time, which means that financial accounting information should be available to those who use it when needed. This is because if the information is not available when needed, or is provided long after the event to which it relates, the information loses its usefulness and thus the effectiveness of the decision. Accordingly. 4. Understandability: Decision makers vary greatly in the types of decisions they make, the decision-making methods they use, the information they have or can obtain from other sources, and their ability to apply this information. For information to be useful, a connection must be established between these users and the decisions they make, and this connection is represented by ease of understanding, which is one of the characteristics of information that allows users to have a reasonable amount of accounting knowledge to understand the meaning of this information, and defines understandability as the ease of understanding accounting information that facilitates the classification, description and presentation of information in a clear and concise manner. It is expected that users of accounting information have a basic understanding of the field of accounting and the commercial and economic aspects of the economic unit, and that they have the desire to make sufficient effort to understand the accounting information presented in the financial reports of the economic unit. The presented monetary data must be simple and free from ambiguity.

17 .The relationship between the quality of accounting information and the efficiency of the financial market

Union points out that financial markets are a fundamental pillar in the financial structure of any economic system, as they play a pivotal role in attracting savings and directing them towards investments that support economic growth and enhance the efficiency of capital allocation. The success of the stock market depends largely on the availability of high-quality financial information, which enables comprehensive and transparent disclosure of the financial position of companies, the results of their activities, their profits, and their future expectations.

In this context, the quality of accounting information is a crucial factor in achieving the efficiency of the financial market, as high-quality accounting information helps determine the true value of traded shares, and provides reliable data that enables investors to make sound investment decisions. The quality of information also contributes to enhancing investor confidence in the market, which leads to increased effectiveness in allocating resources and rationalizing investment decisions.

Thus, the relationship between the quality of accounting information and the efficiency of the financial market is a direct relationship; The higher the quality of accounting information, the greater the market's ability to achieve efficiency in allocating capital, which enhances economic growth and achieves financial stability.

3. Results and Discussion

The definition of financial market efficiency is derived from the following assumed facts:

1. Stock prices quickly depend on new information and must reflect information relevant to the economic unit as a whole.
2. There are a large number of competitors and participants in the market, and information is available quickly and at a low cost.
2. New information must be random and unpredictable, which means that stock prices will also change in an unordered manner in response to this information.
3. All known facts will be reflected in the current cost of the stock, and some new information will only lead to a change in the price.

Therefore, as long as prices reflect certain information quickly and correctly, we can say that financial markets are efficient, and there are many studies that confirm that stock prices will change quickly and correctly with the emergence of new information. Financial markets can be divided into three types:

1. Weak Form: The weak form hypothesis of market efficiency is that the information contained in stock prices is historical information related to changes in the stock price and the volume of transactions that occurred in it in the past, which means that the prediction process depends on studying the variables that occurred in the price in previous days. Past months or years are considered irrelevant, and this is the definition of the weak form in the theory of random motion.
2. Semi-strong Form: Based on the hypothesis, prices in financial markets of a general, historical and current nature are directly affected by all information represented in economic events and announcements related to the economic unit issuing the securities, including acquisitions and mergers, and therefore investors cannot obtain extraordinary profits. 3. Strong Form: The strong form of market efficiency refers to the fact that the current stock price includes all relevant information about the economic unit, whether public or private. The more stringent form includes the assumption that stock prices are unpredictable and that any predictions based on current information and past outcomes will be random, see Table 1.

Table 1. Market Efficiency Levels Assumptions

T	Hypothesis	Proficiency level
.1	**weak form**	**The current stock price reflects all historical information .specifically related to the stock price**
.2	**Semi-strong .form**	**Current stock prices reflect all historical and public stock price .information**
.3	**Strong shape**	**Current stock prices reflect all historical, public and class-specific .information**

Source: Prepared by the researcher

18 .Models for measuring the suitability of accounting information quality

The importance of the quality of accounting information is determined by its ability to explain changes in stock prices or returns, as this relationship is measured using statistical tools such as the coefficient of determination. The coefficient of determination is used to assess the degree to which changes in accounting information can be explained by regression models, where accounting information is considered a dependent variable in the relationship with stock price or returns. When the explanatory power of accounting information in these models decreases, this indicates a decline in the quality of accounting information over time.

Theoretically, stock prices are supposed to reflect the market value of economic units, while accounting numbers represent fixed values based on the accounting procedures and standards followed. When there is a strong relationship between changes in accounting information and changes in market value, this indicates that accounting information is of high quality, as it is relevant, reliable, and able to accurately reflect the financial reality of the economic unit. Therefore, accounting information quality measurement models, such as regression models and coefficient of determination, are effective tools for assessing the relevance of accounting information and its ability to explain changes in market value. These models demonstrate the importance of accounting information in supporting investors' decisions and enhancing the efficiency of financial markets.

On this basis, there are three models to measure the suitability of the quality of accounting information: 1. Return Model: The return model represents the extent to which the basic relationship between returns and changes in stock market prices is verified. This model was developed by (Easton & Harris 1991). It is the first model of value suitability that includes profit levels, profit changes, and profit decomposition through the following, see Table 2.

$$Rit = \beta 0 + \beta 1 EPSit / Pit - 1 + \beta 2 (EPSit - EPSit -1)/ Pit - 1 + eit$$

Table.2 Return Model Equation Codes

The symbol	Code explanation

Right	It represents the annual return (including cash dividends) per share of economic) uniti) for period (t .(
Pit – 1	The share price on the accounting reporting date for the shares of the economic) uniti period (previous year (t-1 .(
EPSit	Represents the annual earnings per share for the current period of the economic . unit
EPSit -1	) It represents the change in annual earnings per share of economic uniti for the ( ) period fromt) the current year to the previous year (t-1 .(

Source: Prepared by the researcher based on what was stated in the above source

2. Price Model: Ohlson's own price model is a widely used model to estimate the relevance of accounting information. It is a linear regression model that expresses the market value of an economic unit (stock price of an economic unit) as a function of its earnings, book value, and related value information. While (Shaheen) indicated that this model describes the relationship between stock price, accounting profit, book value, and operating cash flows, the difference between this model and the return model is that it allows the assessment of the relevance of book value, accounting profit, and operating cash flows simultaneously, while the return model allows the assessment of relevance is assessed taking into account only accounting profit. It takes the following formula, see Table 3.

$$Pit = \beta 0 + \beta 1\ EPSit + \beta 2\ OCF + \beta 3\ SBVit + eit$$

Table.3 Price Model Equation Codes

The symbol	Code explanation
Pt	.economic unit at the end of the financial period
EPSit	Accounting earnings per share at the end of periodt .
SBVit	Book value of equity at the end of periodt-1 .
OCF	Operating cash flows per share at the end of periodt .
et	. error
β	. Beta coefficient of the variable
t	. duration

Source: Prepared by the researcher based on what was stated in the above source

In this model, current income is used as a measure of abnormal returns, while book value is used as a measure of the cash value of expected normal future earnings. According to Olson's model, the market value of the unit is considered a linear function of earnings and book value. This model contains many rules and produces criteria that represent the way in which market values are related to accounting and other relevant information, and the statistical correlation between stock price and earnings is used as a primary means of assessing the value of accounting figures. If the variables related to accounting are relevant to investors, there is a relationship between stock prices, earnings, book value, and operating cash flows, and this is measured using the regression model (R2).

Perhaps the most important difference between the price model and the return model is the following aspects:

1. When using the return model, the relevance of the value decreases due to increased market volatility, which confirms the importance of the price model and that the bias of the return coefficient in the price model is smaller compared to the return model.
2. The main difference between value fit studies that study price levels and value fit studies that study price or return changes is that the former is concerned with determining what the value of the economic unit reflects.
4. The price model takes into account the value of accounting earnings, book values, and operating cash flows, while the return model takes into account only the value of accounting earnings.
5. Stock prices reflect future profit expectations, and stock prices determine earnings.

6. The price model is more effective because it considers all accounting data, unlike the return model that addresses different research questions. The purpose of the price model is to determine the value of the economic unit, rather than reflecting changes in value over a certain period of time.
7. The price model studies the impact of accounting information on the market and stock valuation, and provides a more accurate result of the value of the stock than the return model.

3. Market Participation Model: In highly successful markets, prices are expected to rise rapidly when the original price is updated with information about the intrinsic value of the asset. This market is referred to as an efficient market. The efficiency of information related to stock prices helps investors make decisions regarding their trading strategies that lead to high returns. Market experts study past stock prices in order to predict future prices. In conducting technical analysis, which is the analysis of financial information related to economic units such as earnings, asset values, etc., which aims to help investors choose the stocks they want to buy, see Table 4.

MPSit = ai + B1EPSit + B2DPSit +B3BVPSit + eit

Table. 4 Market Participation Model Equation Code

The symbol	Code explanation
MPSit	Market price per share of the economic uniti at timet .
EPSit	.It is the return per share of the economic uniti at timet .
DPSit	Dividends per share of the economic uniti at timet .
BVPSit	Book value of equity per share in the economic uniti at timet .

Source: Prepared by the researcher based on what was stated in the above source

The price model was chosen to measure the suitability of the quality of accounting information for the following reasons:

1. The most comprehensive model: The price model takes into account the value of accounting profit, book value, and operating cash flows, while the return model takes into account only the value of accounting profit.
2. The most accurate model: The price model is more accurate in estimating the value of the stock than other models
4. The most common model: It is one of the most widely used models by researchers and has proven its high explanatory power in determining the utility of accounting information, see Table 5.

Table. 5 Comparison table between models for measuring the suitability of accounting :information quality

Disadvantages	Advantages	Factors to consider	The model
Does not take into account book .values	Easy to use	accounting profits	Return Model
more complex	More accurate	Accounting profits and book values	Price model
Requires long-term .historical data	takes into account investor behavior	Accounting profits and book values	Market Participation Model

Source: Prepared by the researcher

19 .The relationship between cybersecurity and the quality of accounting information:

Cybersecurity is closely related to the quality of accounting information, as it aims to protect accounting information systems from electronic threats that may affect the reliability and relevance of information. As economic units increasingly rely on

technology and the Internet, their systems have become more vulnerable to hacking and cyber attacks, such as electronic fraud, forgery, and data leakage, which threatens the quality of accounting information and reduces its value .

Cyberattacks contribute to distorting financial statements and weakening confidence in accounting information, which negatively affects the performance of economic units and investment decision-making. Therefore, cybersecurity policies are essential to enhance risk management and protect information assets, as they work to reduce external (such as viruses and hacking) and internal (such as misuse of software and hardware) threats.

Studies have shown that enhancing cybersecurity contributes to improving the quality of accounting information by ensuring the integrity of financial reports and increasing their transparency, which enhances investor confidence and reduces information asymmetry. The use of modern technologies and advanced software also helps protect accounting data and reduce the risks of cyber attacks, which supports the continuity of economic units and increases the relevance and value of accounting information. Ultimately, cybersecurity is a crucial element in maintaining the quality of accounting information, as it provides a secure environment that enables the production of reliable and accurate information, which enhances user confidence and supports sound financial decision-making.

Section Two

Practical Aspect

1 .Overview of Banks Research Sample

The Iraq Stock Exchange is a financial institution for public benefit, established under Temporary Law No. 74 of 2004, and began its activities on June 24, 2004. It succeeded the Baghdad Stock Exchange, which was established in 1991 under Law No. 24, which aimed to regulate the trading of securities, protect the national economy, and promote savings and investment. However, the Baghdad Stock Exchange was closed in 2003 due to war conditions, and the market was later re-established under the name "Iraq Stock Exchange". The Iraq Stock Exchange regulates and monitors the trading of securities, including stocks and bonds issued by the government and joint-stock companies, with the aim of ensuring the safety and accuracy of financial transactions. The market is managed by the Board of Governors, which consists of nine members appointed annually, and their mission is to formulate general policies and supervise market activities. The market is a major channel for attracting investors and directing savings towards investments that support the national economy, without its goal being to make a profit. The market has contributed to enhancing investment development in Iraq by facilitating the movement of funds between individuals, institutions and various sectors.

2. An introductory note about the banks, the research sample

The research sample consists of commercial banks listed in the Iraq Stock Exchange with a number of (10) banks during the period between (2013 - 2022), and the researcher preferred to choose the financial sector from among the rest of the sectors for the following reasons:

1. Most of the economic units listed in the Iraqi market are within the banking sector, as the number of listed banks, according to the reports of the Iraq Stock Exchange, reached (44) banks, including Islamic banks, the number of which is (21)
2. The most economic units trading in shares, and according to the reports of the Iraq Stock Exchange, the volume of traded shares reached (930) billion shares with a financial value of (812 billion Iraqi dinars) during the year 2021.
3. It is the most important and active sector in the Iraqi economy, as the trading volume of the corporate sector reached (95.9%) during the year 2021, according to the reports of the Iraq Stock Exchange, so the banking sector was chosen, which has a number of banks listed in it (23) companies and the research sample

was selected (10) banks after excluding newly established banks and banks whose data was not complete within the time series of the research sample. Table (3-1) summarizes the identification profile of the economic units, see Table 6.

Table. 6 Research Sample

T	Bank name	Founding date	Capital in the year of establishment	Capital in 2022
.1	Commercial Bank	1992/02/11	100,000,000,000	250,000,000,000
.2	Ashur Bank	2005/25/04	25,000,000,000	250,000,000,000
.3	Investment Bank	1993/13/07	100,000,000	250,000,000,000
.4	Gulf Bank	1999/20/10	600,000,000	300,000,000,000
.5	United Bank	1994/20/08	1,000,000,000	300,000,000,000
.6	Mansour Bank	2005/13/09	55,000,000,000	250,000,000,000
.7	Mosul Bank	2001/23/08	1,000,000,000	252,500,000,000
.8	Bank of Baghdad	1992/18/02	100,000,000	250,000,000,000
.9	Sumer Bank	1999/08/07	400,000,000	250,000,000,000
.10	National Bank	1995/01/02	400,000,000	270,000,000,000

Source: Prepared by the researcher based on the Iraq Stock Exchange Bulletin for the year 2022

3.Measuring the relevance of the value of accounting information

The researcher relied on the price model to measure the relevance of the value of accounting information; as it is one of the most widely used models by researchers and has proven the high explanatory power to determine the benefit of accounting information, see Table 7.

The price model is used to measure the relevance of the value of accounting information for the research sample of banks listed in the stock market through the following formula:

$$Pit = \beta 0 + \beta 1\ EPSit + \beta 2\ OCF + \beta 3\ SBVit + eit \quad 3$$

Table .7 Price Model Utilization to Assess the Relevance of Accounting Information Value

Pt	.economic unit at the end of the financial period
EPSit	Accounting earnings per share at the end of periodt .
SBVit	Book value of equity at the end of periodt-1 .
OCF	Operating cash flows per share at the end of periodt .
et	. error
β	. Beta coefficient of the variable
t	. duration

The annual relevance value is measured through the difference between the value of the dependent variable in the price model (stock price) and its predicted value according to the regression equation used, and the smaller the difference, the higher the relevance value, i.e. the independent variables in the price model (profit, cash flow, book value) were highly suitable for predicting the dependent variable (stock price). Therefore, the above equation will be applied using the SPSS statistical program and based on the

information available in the financial statements of each bank in the research sample during the years.(2022-2013)

4 .The impact of cybersecurity on improving the quality of accounting information

In this part of the practical aspect of the research, a questionnaire was relied upon, as it was designed for the purpose of testing the impact of cybersecurity on improving the quality of accounting information. This questionnaire consisted of two axes- :

The first axis is dedicated to measuring the impact of cybersecurity (35) paragraphs distributed into five dimensions classified according to the dimensions of the COBIT framework (19), and the second axis is dedicated to measuring the quality of accounting information, consisting of 24 paragraphs and classified according to the dimensions of cybersecurity, according to the intellectual framework of financial accounting.

The (five-point Likert) scale is used to express five-dimensional sentences, and the measurement range ranges from one point for I completely disagree with the content to five points for I completely agree with the content, as shown in the following table 8:

Five-point Likert scale scores**Table. 8**

I totally disagree	I disagree	neutral	I agree	I totally agree	Response
1	2	3	4	5	Degree

/ The default mean of a five-point Likert scale = (sum of the ratings of the responses above) number of scale categories

The default mean of a five-point Likert scale = (5+4+3+2+ 1)/ 5 = 3 points

(123)questionnaire forms were analyzed by the individuals participating in the sample. The following is a description of the individuals who were selected to participate in the questionnaire.

5 .Description of the questionnaire sample individuals

First: Distribution of sample individuals by gender, see Table 9.

Table. 9 of distribution of questionnaire sample members by gender

Cumulative percentage	ratio	Repetition	Category	variable
37.4	37.4	46	feminine	Sex
100.0	62.6	77	male	
	100.0	123	Total	

Second: Distribution of individuals according to academic qualification

Table.10 of questionnaire sample members according to academic qualification

Cumulative percentage	ratio	Repetition	Type	variable
11	11	14	diploma	Academic qualification
76	65	80	Bachelor's	
96	20	25	Master's	
100.0	3.3	4	PhD	
	100.0	123	Total	

Third: Distribution of individuals according to age group, see Table 10

Table.11 Distribution table of questionnaire sample members according to age group11 table

Cumulative percentage	ratio	Repetition	Category	variable

0.8	.8	1	25-18	Age group
25.2	24.4	30	35-26	
52.8	27.6	34	45-36	
98.4	45.5	56	55-46	
100.0	1.6	2	+55	
	100.0	123	Total	

first axis Internal consistency of the paragraphs of the

Internal consistency table for the paragraphs of the
Table12 first axis - cyber security

Dimensions of the cybersecurity variable					
reinforcement		**Privacy**		**confidentiality**	
Correlation coefficient	**Paragraph**	**Correlation coefficient**	**Paragraph**	**Correlation coefficient**	**Paragraph**
.623 **	**X1**	**.701 ****	**X1**	**.661 ****	**X1**
.582 **	**X2**	**.596 ****	**X2**	**.640 ****	**X2**
.681 **	**X3**	**.683 ****	**X3**	**.618****	**X3**
.726 **	**X4**	**.690 ****	**X4**	**.652****	**X4**
.726 **	**X5**	**.747 ****	**X5**	**.678****	**X5**
.571 **	**X6**	**.694 ****	**X6**	**.664****	**X6**
.707 **	**X7**	**.680 ****	**X7**	**.661****	**X7**
.614 **	**X8**	**.578 ****	**X8**	**.473****	**X8**
****. Correlation is significant at the 0.01 level (2-tailed).**					
***. Correlation is significant at the 0.05 level (2-tailed).**					

Source: Prepared by the researcher

From the table 12 above, it can be noted that all correlation coefficients between the second axis in general and the paragraphs that comprise it had high and statistically significant values. This is evident from the fact that all significance values (2-tailed) were less than (0.05). In addition, all of these values were positive, indicating that there is a direct correlation between each paragraph and the axis to which it belongs. This conclusion reflects the existence of high internal consistency between the paragraphs of that axis. In other words, it can be believed that each paragraph contributed to improving and enriching the variable being measured.

second axis Internal consistency of the paragraphs of the

Table.13second axis - cyber security Internal consistency of the paragraphs of the

Dimensions of the independent variable cyber security					
reinforcement		**Privacy**		**confidentiality**	
Correlation coefficient	**Paragraph**	**Correlation coefficient**	**Paragraph**	**Correlation coefficient**	**Paragraph**
.623 **	**X1**	**.701 ****	**X1**	**.661 ****	**X1**

.582 **	X2	.596 **	X2	.640 **	X2
.681 **	X3	.683 **	X3	.618**	X3
.726 **	X4	.690 **	X4	.652**	X4
.726 **	X5	.747 **	X5	.678**	X5
.571 **	X6	.694 **	X6	.664**	X6
.707 **	X7	.680 **	X7	.661**	X7
.614 **	X8	.578 **	X8	.473**	X8
****. Correlation is significant at the 0.01 level (2-tailed).**					
***. Correlation is significant at the 0.05 level (2-tailed).**					

Source: Prepared by the researcher

From the table 13 above, it can be noted that all correlation coefficients between the second axis in general and the paragraphs composed of it had high and statistically significant values. This is evident from the fact that all significance values (2-tailed) were less than (0.05.) In addition, all of these values were positive, indicating a direct correlation between each paragraph and the axis to which it belongs. This conclusion reflects the existence of high internal consistency between the paragraphs of that axis. In other words, it can be believed that each paragraph contributed to improving and enriching the variable being measured.

The strength of the Pearson Correlation coefficient ranges between positive one and negative one, and the positive sign indicates a direct relationship, while the negative sign indicates an inverse relationship, and the closer the value of the correlation coefficient is to positive one or negative one, the stronger the correlation, and the closer its value is to zero, the weaker the correlation

Table. 14 Cybersecurity Dimensions Summary

Rank	coefficient of variation	Standard deviation	Arithmetic mean	Distance	Paragraph number
2	**0.148**	**0.593**	**4.007**	confidentiality	**1**
1	**0.138**	**0.566**	**4.098**	Privacy	**2**
3	**0.132**	**0.526**	**4.002**	reinforcement	**3**
	0.118	**0.477**	**4.036**	**Dimensions of cyber security**	

Source: Prepared by the researcher

It is clear from the table 14 above that the arithmetic averages expressing the dimensions of cybersecurity ranged between (4.098-4.002), which are highly significant averages. The privacy dimension obtained a high score, and the enhancement dimension obtained the lowest score of the three dimensions, while the general index of cybersecurity reached (4.036), which indicates that cybersecurity is applied to a high degree in the Iraqi banks listed on the stock market.

second axis Internal consistency of the paragraphs of the

Table. 15 Internal consistency table for the paragraphs of the second axis - the quality of accounting information

Dimensions of the variable: Quality of accounting information					
relative importance		**Confirmatory value**		**predictive value**	
Correlation coefficient	**Paragraph**	**Correlation coefficient**	**Paragraph**	**Correlation coefficient**	**Paragraph**
.697 **	**X1**	**.697 ****	**X1**	**.697 ****	**X1**
.682 **	**X2**	**.785 ****	**X2**	**.677 ****	**X2**
.748 **	**X3**	**.687 ****	**X3**	**.809 ****	**X3**
.787 **	**X4**	**.618 ****	**X4**	**.645 ****	**X4**
.778 **	**X5**	**.681 ****	**X5**	**.611 ****	**X5**
.837 **	**X6**	**.721 ****	**X6**	**.725 ****	**X6**
.796 **	**X7**	**.755 ****	**X7**	**.746 ****	**X7**
1		**.668 ****	**X8**	**.742 ****	**X8**
****. Correlation is significant at the 0.01 level (2-tailed).**					
***. Correlation is significant at the 0.05 level (2-tailed).**					

Source: Prepared by the researcher

From the table 15 above, it appears that all correlation coefficients between the third axis and the paragraphs it consists of had high values and statistical significance, as all probability values (2-tailed) were less than 0.05. All of these values were positive, indicating the presence of a direct correlation between each paragraph and the axis to which it belongs, which reflects the high internal consistency between the paragraphs of that axis, and that each paragraph contributed to enriching and saturating the variable being measured.

Table .16 Summary of dimensions of the relevance of accounting information value

Rank	coefficient of variation	Standard deviation	Arithmetic mean	Distance	Paragraph number
1	**0.141**	**0.564**	**3.999**	predictive value	**1**
3	**0.157**	**0.600**	**3.815**	Confirmatory value	**2**
2	**0.162**	**0.626**	**3.869**	relative importance	**3**
	0.140	**0.545**	**3.895**	**Dimensions of suitability**	

Source: Prepared by the researcher

It is clear from the table 16 above that the arithmetic averages expressing the dimensions of the appropriateness of the value of accounting information ranged between (3.999-3.815), which are highly significant averages. The predictive value dimension obtained a high degree, and the confirmatory value dimension obtained the lowest degree of the three dimensions, while the general index of appropriateness reached (3.895), which indicates that accounting information has a highly appropriate value in the banks listed on the Iraq Stock Exchange.

6 .Testing research hypotheses and analyzing results

Main hypothesis: There is a statistically significant impact of cybersecurity in its dimensions on improving the quality of accounting information in its dimensions

To test this hypothesis, the following linear regression model was formulated:-

$$Rel = B_0 + B_1 CS + \varepsilon$$

-:where

CS .The second independent variable (cybersecurity) =

Using theSPSS statistical program : the results were as follows ,

Table.17 Results of testing the impact of cybersecurity on the relevance of accounting information value

Transaction number table					Analysis of variance			Model Summary		
Sig t *	T	Standard error	B	independent variable	Sig F*	Df degree of freedom	F calculated	R ² coefficient of determination	R correlation coefficient	Dependent variable
.000	9.475	.41443	.745	Cyber Security	.000	1.121	89,771	.426	.653	Relevance of accounting information value

Source: Prepared by the researcher

The results in the table 17 show that the value of (R0.653) confirms the direct relationship between cybersecurity and the appropriateness of the value of accounting information. The coefficient of determination reached (0.426), which explains (42.6%) of the variance in the appropriateness of the value of accounting information. It is clear that the value of (F) reaches (89.771) at the significance level (Sig0.000), which confirms the importance of the regression at the level (a≤0.05) and with one degree of freedom. According to the data in the coefficient number table, it can be noted that the value of (B) is (0.745). The value of (T 9.475) is at the significance level (Sig .000), which confirms the importance of the coefficient at the level (a≤0.05). In conclusion, we accept this hypothesis. **This means that the sample data has provided convincing evidence of accepting the hypothesis for the statistically proven effect. Thus, there is a statistically significant (positive) effect of cybersecurity on value fit.**

The following figure 1 confirms the direct relationship between the two variables through .the upward trend of the curve

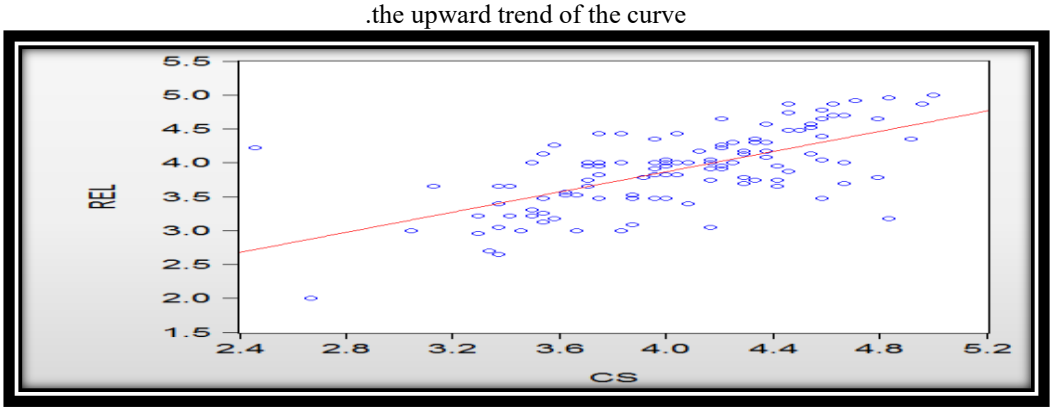

Figure.1 The relationship between cybersecurity and value fit

Based on the results obtained, we can reformulate the regression equation for use in prediction. According to the table shown, the regression equation is as follows:-

$$\text{Rel} = 890 + 0.745 * \text{CS} +$$

The following figure 2 illustrates the criteria for testing regression analysis in the form of graphs, where the distribution of points around the straight line is depicted and the statistical residuals follow the normal distribution.

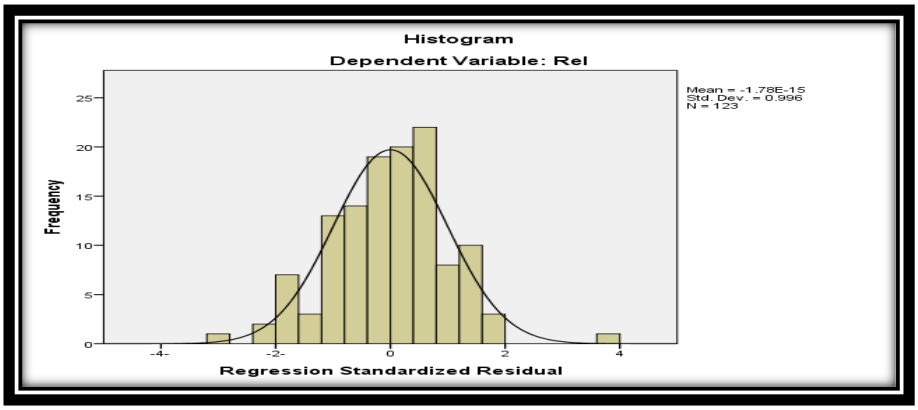

Figure.2 Frequency histogram of the residuals of the second main hypothesis

The figure 3 below illustrates how the regression analysis test is completed graphically, indicating the distribution of points around the straight line and demonstrating that the statistical residuals are consistent with a normal distribution, while also illustrating the fulfillment of the two requirements of the analysis.

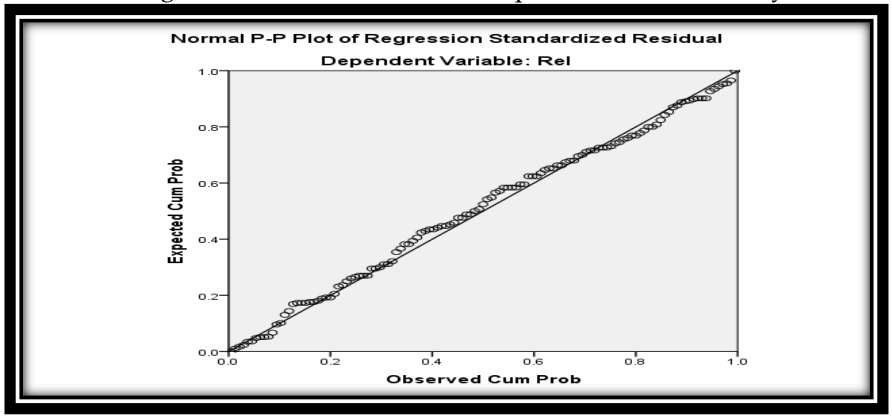

Figure.3 The normal distribution of the residuals of the second main hypothesis

4. Conclusion

1. Enhancing the reliability of accounting information Cybersecurity plays a pivotal role in enhancing the reliability of accounting information by protecting data from hacking and cyber threats. This increases users' confidence in the accuracy and integrity of financial statements.
2. Improving transparency and credibility The implementation of effective cybersecurity systems contributes to enhancing transparency and credibility in accounting information, as it reduces the risk of data manipulation or leakage, which enhances the confidence of investors and stakeholders.
3. Increasing the confirmatory value of information Cybersecurity increases the confirmatory value of accounting information by ensuring the integrity and accuracy of data, making it more suitable for making economic and financial decisions.
5. Enhancing the predictive value of information Thanks to cybersecurity, accounting data becomes more secure and accurate, which enhances its ability to provide reliable financial forecasts that help in strategic planning and making future decisions.
6. Attracting investments Cybersecurity is an attractive factor for domestic and foreign investments, as it ensures a safe and transparent business environment, which increases investor confidence in economic units.
7. The role of IT governance as a supporting factor Although the research focuses on cybersecurity, IT governance is considered a supporting factor in enhancing the effectiveness of cybersecurity systems, which is positively reflected in the quality of accounting information.
8. Providing a safe work environment Cybersecurity contributes to providing a safe work environment that allows information to flow safely and effectively, which is positively reflected in the quality of accounting information and its ability to meet users' needs.
9. Reducing financial and legal risks Cybersecurity reduces financial and legal risks resulting from electronic breaches, which preserves the reputation of economic units and reduces potential financial losses.

Recommendations

1. Strengthening cybersecurity systems Banks and economic units should invest in advanced and effective cybersecurity systems to protect financial and accounting data from electronic threats, which enhances the quality of accounting information.
2. Raising awareness of the importance of cybersecurity Workshops and training courses should be held for employees of economic units to raise their awareness of the importance of cybersecurity and how to apply it correctly to protect data.
3. Adopting international standards for cybersecurity It is recommended to adopt recognized international standards in the field of cybersecurity, such as ISO/IEC 27001, to ensure the application of best practices in information protection.
4. Enhancing cooperation between stakeholders Cooperation should be enhanced between government agencies, the private sector, and financial institutions to exchange experiences and knowledge on the best ways to implement cybersecurity.
5. Developing IT governance policies Clear IT governance policies should be developed to support cybersecurity systems, which contributes to enhancing the quality of accounting information.
6. Conducting periodic audits It is recommended to conduct periodic audits of cybersecurity systems to ensure their effectiveness and efficiency in protecting accounting data.
7. Providing the necessary funding Adequate funding should be provided to support cybersecurity projects and develop the necessary technological infrastructure to ensure data protection.

8. Enhancing transparency and disclosure Economic units should enhance transparency in disclosing the cybersecurity procedures followed, which increases the confidence of investors and stakeholders.
10. Establish specialized cybersecurity teams It is recommended to establish specialized cybersecurity teams within economic units to monitor cyber threats and respond to them quickly and effectively. 10. Promote research and development Research and development in the field of cybersecurity should be encouraged to keep pace with continuous technological developments and increasing cyber threats.

REFERENCES

[1] M. M. Al-Sartawi, "Information technology governance and cybersecurity at the board level," Int. J. Crit. Infrastruct., vol. 16, no. 2, pp. 150–161, 2020.

[2] A. T. M. Q. Mohamme, "Article Review: Using Cybersecurity in Digital World," Dirasat Tarbawiya, vol. 16, no. 62, 2023.

[3] J. Pande, "Introduction to cyber security," Technology, vol. 7, no. 1, pp. 11–26, 2017.

[4] M. J. D. B. M. De Alte, "The effects of Global Financial Crisis on the Value Relevance of accounting information: Portuguese evidence," 2014. [Online]. Available: https://repositorio-aberto.up.pt/bitstream/10216/75610/2/32445.pdf

[5] L. A. Beisland, Essays on the Value Relevance of Accounting Information, Bergen, Norway: Norwegian School of Economics and Business Administration, 2008.

[6] M. Rani, "The effects of audit committee characteristics on the value relevance of accounting information in New Zealand," Doctoral Dissertation, Auckland Univ. of Technology, 2011.

[7] M. E. Barth, W. H. Beaver, and W. R. Landsman, "The relevance of the value relevance literature for financial accounting standard setting: another view," J. Account. Econ., vol. 31, no. 1–3, pp. 77–104, 2001.

[8] M. H. Keener, "The relative value relevance of earnings and book value across industries," J. Finance Accountancy, vol. 6, pp. 1–10, 2011.

[9] N. Azar, Z. Zakaria, and N. A. Sulaiman, "The Quality of Accounting Information: Relevance or Value-Relevance?," Asian J. Account. Perspect., vol. 12, no. 1, pp. 1–21, 2019.

[10] J. D. Spiceland, M. W. Nelson, and W. B. Thomas, Intermediate Accounting, 9th ed. New York, NY: McGraw-Hill Education, 2018.

[11] IASB, Conceptual Framework for Financial Reporting, London, UK: Int. Account. Standards Board, 2018.

[12] P. D. S. Costa, A. F. Pinto, F. M. Nunes, and S. Lemes, "Comparability of accounting choices in the statement of cash flow: Evidence from Brazil," Contaduría y administración, vol. 64, no. 3, 2019.

[13] J. B. Khanagha, "Value relevance of accounting information in the United Arab Emirates," Int. J. Econ. Financ. Issues, vol. 1, no. 2, pp. 33–45, 2011.

[14] Securities Commission, "Instructions for Trading in Securities," 2015.

[15] Securities Commission, "Daily and Weekly Bulletins," 2022.

[16] A. A. Rafiei and A. M. Behrooz, "The Effect of Business Intelligence on the Quality of Accounting Information," Management Science Letters, vol. 10, no. 2, pp. 473–480, 2020.

[17] Y. Rezaee and A. Wang, "The impact of information technology on the quality of accounting information," Journal of Accounting and Public Policy, vol. 40, no. 3, p. 106767, 2021.

[18] Y. Yekini, A. Yekini, and L. Adebisi, "Effect of cloud computing on accounting practices," International Journal of Finance and Accounting, vol. 4, no. 4, pp. 240–245, 2015.

[19] A. Elbardan and H. Ali, "Integrating ERP and business intelligence for improved accounting information quality," Journal of Enterprise Information Management, vol. 30, no. 2, pp. 263–284, 2017.

[20] N. Mohammed and A. A. Khalid, "The Impact of Cybersecurity on the Quality of Accounting Information: A Study on the Jordanian Banking Sector," International Journal of Academic Research in Accounting, Finance and Management Sciences, vol. 11, no. 2, pp. 107–118, 2021.

[21] L. D. Smith, "Cybersecurity issues in accounting," Journal of Accountancy, vol. 217, no. 6, pp. 30–36, 2014.

[22] M. L. Granlund, "Accounting information quality and cybersecurity assurance: Conceptual framework," Information & Computer Security, vol. 29, no. 3, pp. 455–472, 2021.

[23] D. E. Rouse, "The Interconnection Between Financial Information and Cybersecurity," CPA Journal, vol. 89, no. 2, pp. 18–25, 2019.
[24] D. Brown-Liburd and V. Vasarhelyi, "Big Data and Audit Evidence," Journal of Emerging Technologies in Accounting, vol. 12, no. 1, pp. 1–16, 2015.
[25] C. H. Fearnley and B. Beattie, "Auditor reporting and cybersecurity risk," Accounting and Business Research, vol. 45, no. 6–7, pp. 705–729, 2015.
[26] B. A. Payne and R. Curtis, "Cybersecurity Threats and the Future of Financial Reporting," Strategic Finance, vol. 98, no. 3, pp. 29–36, 2016.
[27] A. Zhang, Y. Zhang, and J. Liu, "Blockchain-based accounting information systems: Research framework and future directions," International Journal of Accounting Information Systems, vol. 38, p. 100501, 2020.
[28] P. B. Lowry, J. Zhang, and C. Wu, "Protecting Accounting Information Systems with Machine Learning and Artificial Intelligence," Decision Support Systems, vol. 124, p. 113097, 2019.
[29] R. Davis, "Cybersecurity and its effect on accounting information," Accounting Today, vol. 30, no. 9, pp.
[30] T. O. Gilbert, "Digital assurance and cybersecurity in modern financial reporting," Financial Executive, vol. 33, no. 1, pp. 36–40, 2017.
[31] H. M. Abdel-Basset, "Cybersecurity and financial reporting: a review," International Journal of Disclosure and Governance, vol. 17, no. 4, pp. 240–255, 2020.
[32] D. R. Kandiah, "Cybersecurity audit and the future role of accounting professionals," Accounting Perspectives, vol. 16, no. 2, pp. 109–126, 2017.
[33] Y. Wang and X. Xu, "Accounting Information System Security and Cybersecurity Assurance," Information Resources Management Journal, vol. 31, no. 3, pp. 20–37, 2018.
[34] J. Kim and J. Lee, "Cyber Threats to Accounting Information Systems and Controls," Journal of Accounting and Organizational Change, vol. 13, no. 2, pp. 130–150, 2017.
[35] R. T. Rust, "The Role of IT in Accounting and Financial Reporting," MIS Quarterly Executive, vol. 12, no. 1, pp. 45–59, 2013.
[36] R. Marston, "Cyber risk and accounting: Threats to corporate reporting," Corporate Communications: An International Journal, vol. 22, no. 3, pp. 305–322, 2017.
[37] J. F. O'Connor, "Internal controls and cybersecurity: Accounting's new frontier," Internal Auditor, vol. 71, no. 4, pp. 40–46, 2014.
[38] F. Al-Bar and M. M. Hoque, "Cybersecurity threat analysis in financial reporting systems," International Journal of Accounting Information Systems, vol. 39, p. 100525, 2021.
[39] A. L. Quinn and M. P. Parker, "Cybersecurity preparedness in audit and assurance: Evidence from Big Four Firms," Accounting Horizons, vol. 34, no. 2, pp. 29–50, 2020.
[40] S. M. Smith and T. S. Johnson, "Enhancing cybersecurity governance for financial information integrity," Information Systems Management, vol. 37, no. 4, pp. 312–325, 2020.
[41] T. L. Anderson, "The cybersecurity-accounting interface: professional implications," Journal of Information Systems, vol. 32, no. 2, pp. 77–95, 2018.
[42] A. T. Ng, "Cybersecurity: accounting implications and governance strategies," International Journal of Accounting & Information Management, vol. 27, no. 1, pp. 1–15, 2019.
[43] A. S. M. Al-Omari and R. M. Al-Sayyed, "The impact of cybersecurity measures on the accounting information system effectiveness," International Journal of Advanced Computer Science and Applications, vol. 11, no. 5, pp. 250–257, 2020.
[44] E. R. George and L. J. Timothy, "IT Governance and Accounting Information Systems," Journal of Information Systems, vol. 35, no. 1, pp. 22–36, 2021.
[45] G. B. McCarthy and P. O'Connell, "Information assurance and the role of accountants," Journal of Emerging Technologies in Accounting, vol. 10, no. 1, pp. 95–112, 2013.
[46] A. E. Green, "Digital transformation and cybersecurity in accounting," Accounting Technology, vol. 29, no. 6, pp. 60–65, 2015.
[47] L. J. Reed and M. S. Griffith, "Cybersecurity Awareness and Controls in Accounting," Management Accounting Quarterly, vol. 18, no. 2, pp. 35–48, 2017.
[48] P. W. Carey and J. E. Goh, "Accountability in Cybersecurity Risk Management," Auditing: A Journal of Practice & Theory, vol. 39, no. 1, pp. 1–19, 2020.

[49] R. T. Vance and B. J. Smith, "Cybersecurity disclosure and financial statement quality," Accounting Review, vol. 94, no. 3, pp. 261–288, 2019.
[50] B. K. Lee and M. S. Carter, "The evolving role of accountants in cybersecurity assurance," Journal of Accountancy, vol. 222, no. 4, pp. 25–31, 2016.
[51] M. G. Yang and L. T. Chen, "Cybersecurity risk and audit response," Journal of Accounting Research, vol. 57, no. 5, pp. 1253–1285, 2019.
[52] N. R. Patel and K. D. Singh, "Cybersecurity and the audit process: risk-based approaches," Managerial Auditing Journal, vol. 35, no. 6, pp. 809–830, 2020.
[53] R. Alsharari, "Cybersecurity governance in accounting: a conceptual framework," International Journal of Accounting & Information Management, vol. 28, no. 2, pp. 217–232, 2020.
[54] Y. Xu and R. Rohde, "Cybersecurity threats and financial reporting risk: an analysis of SEC comment letters," Journal of Information Systems, vol. 33, no. 3, pp. 23–45, 201