International Journal of Studies in Business Management, Economics and Strategies
Volume 3, Issue 8, August - 2024
ISSN (E): 2949-883X
Scholarsdigest.org

SECURITY RISKS CYBER AND ITS EFFECT ON FINANCIAL STABILITY IN COMPANIES CONTACT

1 Sarah Fouad Muslim
Al-Imam Al-Sadiq University, College of Administrative Sciences
sara.fouad@ijsu.edu.iq

2 Zahraa Abdelkareem Mohammed
Al-Imam Al-Sadiq University, College of Administrative Sciences
zahraa_abdalkareem@ijsu.edu.iq

Hussein Ali Hussein Altimimi 3
Al-Mustaqbal University, College of Administrative Sciences
ha723223@gmail.com

Abstract
The research aims to: Identify cybersecurity applications, and their dimensions, and explain their impact on financial stability in telecommunications companies
To reach the feasibility of this technology and achieve the objectives of the study, the descriptive approach was adopted for the theoretical aspect, while the practical aspect was based on conducting a directed questionnaire. For a category of accountants and auditors in various sectors, Then the results were analyzed and the results were presented and analyzed. This study concluded that: There is an effect With indication Statistics when level Morale ($\alpha \leq 0.05$) between administration Risks Security Cyber and to support Stability Financial in Companies Communications And also preparing high-quality financial reports is critical to increasing management control and avoiding opportunistic decisions plays a vital role in the ability to attract money. By comparing the quality of the company's financial reports with those of other companies.

Keywords: Cyber Security, Financial Reports, Financial Statements, Financial Stability.

Introduction

The business environment has recently witnessed major scientific and technological developments in the field of industries, services, and information technology, as well as contemporary developments in administrative sciences. New concepts have emerged such as globalization, intense competition, and the customer's need for high-quality services and products, among others, which constitute challenges and pressures faced by most units in all institutions. These challenges are represented by new requirements that require management to take all measures and follow contemporary administrative methods and policies related to information security and maintaining confidentiality to respond to these challenges.

Security is also the cornerstone of any society, as no activity can take place in the absence of security, whether at the technical level or the legal level, security has become, with the information revolution and cyberspace, an essential part of the services sector that constitutes an added value and a basic pillar for the activities of governments and individuals, such as applications related to e-government, e-health, distance education, e-payment system, and e-commerce. (Zureikat, 2022:1)

Financial reports are the primary means of disclosure to stakeholders, which aims to: Deliver high-quality information to decision-makers, as many parties rely on these reports. From this standpoint great role of the quality of financial reports is clear, which economic units must apply according to methods and techniques to maintain the security of information from any unauthorized deletion or distortion. No doubt imagine what economic units can achieve by applying this technology and the amount of positivity that will be achieved, hence this study came to investigate the impact of applying cybersecurity technology on the quality of financial reports. (Abadi, 2023:1)

1.1 research problem:

As a result of the developments in the technological field and the emergence of new electronic methods and techniques that work onbreakthroughLarge companies that enable hackers to steal and manipulate their financial reports, as it constitutes to risk cyber attacks pose major risks to financial software and applications accuracy of the reports it produces, and this is particularly evident as threat actors continue to target vital business applications that contain huge amounts of financial data for the company, employees, and customers, and the resulting reliable financial reports for investors, shareholders, banks, contributors, and all beneficiaries. Thus, the problem can be formulated as follows:

- Is There an impact of security risks? Cyber and its implications for financial stability in Companies?
- How Cybersecurity Application Helps Business Management Achieve Effective Control and ProtectionFull to repel Cyber attacks to ensure the integrity of financial reportsIraqi?

1.2 Research objectives:

The main objective of the research is to determine the impact of security applications in improving the quality of financial reporting, And this branch's offset goal

1- Learn about cybersecurity applications and dimensions
2- Learn about the concept of financial stability
3- Determine the impact of security ApplicationsCyber financial reports
4- Determine to what extent it affectsApplicationsCybersecurity indirectly on fees Review of financial statements through audit risks.

1.3 Importance of Research:

lies Importance Scientific For this the study in Expose it For the topic important in area Censorship And systems Information accounting, And he is effect application Cybersecurity software on financial stability in Companies Contact and try investigation addition Simple And humble For the library Arabic While Related With its variables.

The importance also stems from the Search for important Risks Cyber that increased Recently The last by the increase in Technology development Information communications and transformations Digital And try Framing Releases Professional Disclosure on Risks Cyber And seeking help in an attempt To limit these Risks In the telecommunications sector. as lies importance This is amazing the study in Being from Few Studies-According to science researcher-that I ate this the topic in the Communication environment,

1.5 Research hypotheses:

- **hypothesisProof:** The presence of a significant effect for risksCyber SecurityOn financial stability inUnitsEconomic.

- **Null hypothesis**: No effect with indication Morale For risks Security Cyber on For stability Financial in Units Economic.

Previous studies

The study sample included a group of accountants and auditors in many government departments, including Iraqi telecommunications companies, in addition to many auditors in the Financial Control Bureau. distribution Questionnaire on sample Random I reached (90) category from staff in Companies Communications

Previous studies

First study	Abrahams,et.al, 2024))
the address	Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security
The problem	Accounting and cybersecurity integration is more than simply a practical requirement—it's a holistic strategy to fortify the foundations of data protection and financial integrity. By exploring the subtleties of this mutually beneficial connection, we hope to shed light on the many facets that make up the contemporary paradigm of financial data security. Any successful organization's cornerstones are accurate financial reporting, open disclosure, and stakeholder confidence..
the goal	The goal of the study is to show how accounting and cybersecurity work together to safeguard financial security and maintain data confidentiality. It seeks to investigate the strategic alignment needed to strengthen companies against the growing dangers posed by cyber threats to sensitive financial information by concentrating on the junction of these two sectors.
Study community and sample	number of business organizations
Results	To successfully reduce these risks, a complete strategic strategy that combines accounting procedures with cybersecurity safeguards is required. This analysis also looks at modern tools and technology that make it easier to integrate cybersecurity and accounting, improving an organization's capacity to recognize, stop, and respond to cyberthreats.
Second study	Sari, et, al,2024))
the address	Determinant Factors of Cyber Security Disclosure: A Systematic Literature Review
Study problem	Disclosure of cybersecurity as a risk factor is especially crucial. Decisions about cybersecurity disclosure are becoming more and more significant due to the annual amount of data breaches that raise serious questions about the cybersecurity plans of businesses. Data breaches can have expensive consequences. However, there is currently a dearth of studies on cybersecurity disclosure.
the goal	The purpose of this study is to determine the variables influencing cybersecurity disclosures. Reviews were conducted on articles from several international publications. A review of the literature was done to identify the crucial elements influencing cybersecurity disclosures.
Study sample	Sample of business organizations

Results	The findings indicate that prior cybersecurity incidents and breaches, peer breaches, public interest, work-from-home policies, board size, independence, gender diversity, institutional shareholders, foreign shareholders, capital expenditures, intangible assets, company growth, size, leverage, profitability, loss, industry, direction, technology committee, and executive change are the most important factors for cybersecurity disclosures.
The third study	Akinyele, Daniel, 2024))
the address	Building a culture of cybersecurity awareness in the financial sector
Study problem	In the current digital era, fostering a culture of cybersecurity awareness in the banking industry is crucial. Financial institutions need to put cybersecurity first in order to safeguard sensitive client data, uphold confidence, and guarantee the stability of the financial system as cyber attacks grow more sophisticated and common.
the goal	The essential components of creating such a culture inside the financial industry are outlined in this short. The need of cybersecurity knowledge is emphasized at the outset of the brief, along with the changing threat landscape and the repercussions of security breaches in the financial industry. After that, it describes the essential actions to establish a cybersecurity awareness culture.
Study community and sample	number of business organizations
Results	Governance and leadership are essential. The secret to success is creating a solid cybersecurity strategy and policy structure, selecting committed cybersecurity leadership, and guaranteeing board involvement.
First study	Abrahams,et.al, 2024))
the address	Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security
The problem	Accounting and cybersecurity integration is more than simply a practical requirement—it's a holistic strategy to fortify the foundations of data protection and financial integrity. By exploring the subtleties of this mutually beneficial connection, we hope to shed light on the many facets that make up the contemporary paradigm of financial data security. Any successful organization's cornerstones are accurate financial reporting, open disclosure, and stakeholder confidence..
the goal	The goal of the study is to show how accounting and cybersecurity work together to safeguard financial security and maintain data confidentiality. It seeks to investigate the strategic alignment needed to strengthen companies against the growing dangers posed by cyber threats to sensitive financial information by concentrating on the junction of these two sectors.
Study community and sample	number of business organizations
Results	To successfully reduce these risks, a complete strategic strategy that combines accounting procedures with cybersecurity safeguards is required. This analysis also looks at modern tools and technology that make it easier to integrate cybersecurity and accounting, improving an organization's capacity to recognize, stop, and respond to cyberthreats.
Second study	Sari, et, al,2024))
the address	Determinant Factors of Cyber Security Disclosure: A Systematic Literature Review
Study problem	Disclosure of cybersecurity as a risk factor is especially crucial. Decisions about cybersecurity disclosure are becoming more and more significant due to the annual amount of data breaches that raise serious questions about the cybersecurity plans of businesses. Data breaches can have expensive consequences. However, there is currently a dearth of studies on cybersecurity disclosure.
the goal	The purpose of this study is to determine the variables influencing cybersecurity disclosures. Reviews were conducted on articles from several international publications. A review of the literature was done to identify the crucial elements influencing cybersecurity disclosures.
Study sample	Sample of business organizations
Results	The findings indicate that prior cybersecurity incidents and breaches, peer breaches, public interest, work-from-home policies, board size, independence, gender diversity, institutional shareholders, foreign shareholders, capital expenditures, intangible assets, company growth, size, leverage, profitability, loss, industry, direction, technology committee, and executive change are the most important factors for cybersecurity disclosures.

The third study	Akinyele, Daniel, 2024))
the address	Building a culture of cybersecurity awareness in the financial sector
Study problem	In the current digital era, fostering a culture of cybersecurity awareness in the banking industry is crucial. Financial institutions need to put cybersecurity first in order to safeguard sensitive client data, uphold confidence, and guarantee the stability of the financial system as cyber attacks grow more sophisticated and common.
the goal	The essential components of creating such a culture inside the financial industry are outlined in this short. The need of cybersecurity knowledge is emphasized at the outset of the brief, along with the changing threat landscape and the repercussions of security breaches in the financial industry. After that, it describes the essential actions to establish a cybersecurity awareness culture.
Study community and sample	number of business organizations
Results	Governance and leadership are essential. The secret to success is creating a solid cybersecurity strategy and policy structure, selecting committed cybersecurity leadership, and guaranteeing board involvement.

2. Literature Review

2.1 Cyber security:

The basis of the emergence of the word cyber(Cybernetic) is associated with the Greek word which means guidance. Control is derived from the word (Kybernetes), meaning the person who steers the ship, as it is used metaphorically for the controller (governor), and thus we can say that cyber is a remote control, as when it comes to another word it means controlling or managing it (Gegan, 2021).

Cyber security is also found in English. (Cyber security), which includes two words, the first is cyber"Cyber" is Latin in origin and means information space, while the second is Security, which means security. Thus, what is meant by cyber security is information space security. If cyber security means information security, it is a more comprehensive and general term. From information security, (Adly, 2021: 187) As a result, cybersecurity can be defined as a collection of technical, organizational, and administrative tools that are used to stop illegal use, misuse, and recovery of electronic data, communications, and information systems. It also improves the security, privacy, and confidentiality of personal data and takes all required precautions to shield citizens and customers from risks in cyberspace. (Adly, 2023: 455)

He knows itCyber Security CenterNational in the United Kingdom (2021 Protection against theft or damage to devices, services, and networks, including the information contained within them.

Cybersecurity is a branch of technology that aims to protect systems. Networks and programs are digital attacks that usually aim to access, change, destroy, or blackmail sensitive information. Cybersecurity is also called "computer security" or "information security."Urethra, 2024:52)

Cybersecurity is a concept that expresses a set of mechanisms. The procedures, methods, and frameworks that aim to protect software and computers from attacks, breaches, and threats to the information they contain. (Gab God, 2021:49)

Cybersecurity can be defined as the security of networks, information systems, data, and information. And devices connected to the Internet. Accordingly, it is the field that relates to the procedures, measures, and protection standards that must be taken or adhered to to

confront threats, prevent violations, or limit their effects in the most severe and worst cases. (Abu Hussein, 2021: 18)

As defined by the International Organization for Standardization, cybersecurity or cyberspace security is as follows:: "Maintaining the confidentiality, integrity and availability of information in cyberspace. Cyberspace has been defined as the complex environment resulting from the interaction of people, programs, and services on the Internet via the technology of devices and networks connected to it, none of which exists in a physical form."

2.2The importance of cyber security:

The importance of cybersecurity can be explained through the following: (Mansour 2021: 226-228(, (Othmani 2019: 19), (Hamoud, 2023), (Issa, 2022: 29)

- Helps avoid fines and penaltiesLawmakers are increasingly enacting legislation that protects the security and privacy of personal data collected by private companies and organizations. Violation of these laws can result in severe fines and penalties.
- Protect the organization's reputationAn organization experiencing a data breach will damage its reputation, and trust between the organization and its customers will be disrupted. Enhancing data management capabilities for most organizations operating in technology information.
- Raising the readiness of the infrastructure to confront any cyber attacks being exposed suddenly.
- Working to provide the basic requirements necessary to reduce risks of cybercrimes targeting users and reducing their impact when exposed to any attacks.
- Work to eliminate any weaknesses that could serve as there are loopholes in computer systems and mobile devices of various types. Therefore, cybersecurity aims to close loopholes in information security systems, in addition to resisting
- Improve the organization's image organizations that have invested significant time and resources into maintaining compliance with industry data security guidelines are often reluctant to partner with organizations that have not done the same.
- Promote the organization's culture of information security organizations that collect data from their customers have a unique opportunity to enhance their culture by adopting advanced security compliance measures that meet or exceed applicable standards or regulations. With it.
- Security compliance supports access controls and accountability. An effective IT security compliance system ensures that only individuals with appropriate credentials can access secure systems and databases that contain critical customer data.
- Working to provide a safe environment for all groups exposed to attacksCyber, to achieve a reliable level of security in conducting transactions in the information society.

Al-Sumaih (2020) summarized the importance of cybersecurity as follows::

1. Maintaining the integrity, consistency, and consistency of information by ensuring data confidentiality and availability.And its readiness when needed.

2. Protect devices and networks as a whole from hacking to be the first line of defense for data and information
3. The ability to detect and address vulnerabilities in the equipment used.
4. . Use and develop open-source tools to achieve cybersecurity principles.
5. Creating a safe working environment when dealing with cryptocurrencies.

2.3 Security dimensionsYesRani:

(Salem, 2022: 74), (Ali, 2023: 120), (Al-Ayeb, 2023: 7)

1. Military dimensionThere is no doubt that cyberspace has become one of the most important primary domains for military operations, such as the land domain. And the sea and space and many countries are increasing their spending on building and enhancing their cyber capabilities. Cyberspace has become an important place in national security strategies, and military strategies in the world today. Many researchers believe that this heralds the beginning of what is called the digital arms race.
2. 2. The political dimension is embodied in upholding the state's political entity, safeguarding the paramount interests, and honoring national symbols and constants that the majority of the populace has agreed upon. It also means refraining from working toward a non-national agenda or obtaining sponsorship from outside parties, despite any excuses or justifications, and exercising freedom of expression in compliance with the laws and rules that ensure it, as well as through nonviolent means that consider the safety and stability of the nation.
3. The economic dimension: this seeks to meet basic needs, give people the means to live decent lives, and raise the level of services while also trying to make living conditions better and provide employment opportunities for people who are of working age. It also considers how people develop their abilities and skills through programs for education, training, and rehabilitation, as well as how to open up opportunities for self-employment within the framework of laws that are able to keep up with the needs of the modern world. (Comparative, 2020, 1)
4. Social dimensionCybercrime causes many harms and negative effects on society, as it depends mainly on impersonating the victim in his financial and social dealings, these effects are not limited to individuals but also extend to organizations and companies, and governments are attractive targets for cybercriminal acts, and these crimes aim primarily to cause many damages to society as a whole.
5. Media dimension: Various media outlets play a major role in educating society about the use of modern technology for detection. Regarding cybercrimes, to be careful not to fall victim to direct and targeted cyber attacks, one must deal with caution, take precautions, and raise the level of security and awareness, such as: setting a strong password, updating devices according to the latest modern technology, and directing members of society towards using modern technology properly, by creating awareness television programs, and distributing awareness brochures through print or electronic newspapers, or social media.
6. Educational dimensionFocusing on creating a generation specialized in the field of cybersecurity is necessary, to work as specialists in this field, which is one of the modern and important fields for confronting transcontinental cyber attacks in this large cyberspace.

7. Legal dimension: Individual, institutional, and governmental activities in cyberspace have legal consequences in the form of rules.The legal framework that regulates transactions in cyberspace and resolves disputes arising from them. Many practical methods have emerged in the use of information technology, such as creating blogs and online communities, the right to protect the ownership of software, and reporting violations and cybercrimes. This has led to the need for legal legislation that is compatible with the changes that have occurred. There is no doubt that legal disputes will affect advertising that is based on the spectrum of Internet users based on their research interests or the sites they visit, breaches and leaks of personal and financial data, whether intentional or unintentional, and the responsibilities of the entity that owns or manages it, and the right to correct and delete personal data. (Al-Shammari,2021:71)

2.4 The concept of financial stability

Interest in the concept of financial stability began in general after the Asian crisis in 1997 and more so after the global financial crisis in 2008, due to the severity of the global financial crisis and the extent of the measures to address it, which led to a new reflection on the responsibility of central banks in detecting and resolving crises and enhancing their role in achieving financial stability., It is necessary to focus on financial stability to achieve economic growth because most transactions in the real economy are carried out through the financial and banking system. Therefore, financial stability is a broad concept that includes different aspects of the financial system. Financial stability has been defined as the state in which the financial system can attract and allocate monetary assets efficiently, as well as absorb "shocks" without harming the real economy. Meaning (avoiding crises) (Simsim, 2022: 51)

Financial stability is defined as the state in which the financial sector can hedge against crises, in addition to its ability to continue performing the function of directing funds to investment efficiently when crises occur, and also to continue making payments efficiently, quickly, and on time. (Al-Asadi, 2022: 36)

It is also defined as "avoiding falling into financial crises, the efficiency of financial and economic resources and their geographical distribution according to financial transactions (savings, investment, loans) (and economic aspects) wealth accumulation, and GDP growth addition to administrative operations such as (financial risk assessment)(Liquidity management) and its distribution through confirmationWorking on the safety and strength of the components of the financial system(Al-Sharifi, 2022: 51)

2.5The importance of financial stability

Most central banks employ a special unit that focuses on financial stability by issuing reports and studies and issuing warnings and alerts. Among the initiatives that can be mentioned are: (Al-Saidi, 2020: 38).

A. Financial stability contributes to the application of best banking practices.
B. Financial stability is a necessary condition for the development of the financial system.
C. Financial stability is a fundamental pillar of economic growth.
D. Financial stability contributes to increased financial inclusion and economic development.
E. The International Monetary Fund has created a map that attempts to predict crises before they occur.

F. The IMF has begun issuing a periodic report twice a year in which it attempts to monitor financial tensions to contain them and limit their spread.

2.6 General concept of financial reports

Financial reports are one of the most important primary sources that provide investors and other users with important information, this importance has increased in light of the globalization of financial markets, the development of communication and publishing methods, and the presence of entities working to prepare high-quality standards. Financial reports, including financial and explanatory statements, are also considered the primary means of communication between the unit's management and users of financial reports, as they contain the progress of activities in the facility and translate them into the form of quality information through which the investment decision can be rationalized and thus the volume of trading in financial markets can be increased, which leads to the activation of those markets, which has an economic return on the country. Abdullah, 2024:891).

According to what was reported, the financial statements are considered part of the financial reports, as they are prepared by the economic units. To meet the increasing requirements and needs of its users, it is practically difficult in today's business environment to achieve these requirements and needs through basic financial statements only due to the large amount of accounting and non-accounting information (Al-Bashir, 2016: 88). Financial reports were also referred to as a unified method for data related to the assets and financial position of the unit and the results of its operations, as financial reports are prepared based on financial accounting data (Al-Hajjami, 2024: 60).

It can be said that financial reports are broader and more comprehensive than financial statements, which are part of the contents of financial reports, as financial reports include all information directly and indirectly related to information, and the lists are the main axis of reports. As for the quality of financial reports, the concepts have varied among researchers (Hatim, 2024:51)

.(2015:29, Habib & Jiang, see it as providing more information about the characteristics of the company's financial performance that are considered appropriate for making certain decisions by certain decision-makers.

It can also be defined as "fulfilling a set of objective or judgmental standards, and it is difficult to measure."This quality is not directly but is evaluated in a "judgmental" way.(2016:7, Goodbye & Imene)

While he sees (1-2014Ferrero Financial reporting is not just an end product as quality in the financial reporting process depends on every part of the process including disclosure of the company's transactions and information related to the selection and application of accounting policies, i.e. providing all the necessary information in a way that helps the user in making decisions. He stressed that quality refers to the credibility of the information provided in the financial report. He also defined it (Seiyaibo & Okoye, 2020:60) as the extent to which financial statements can provide true and fair information about the basic performance and financial position that satisfies all stakeholders (Bandara2020) indicated that quality is the extent to which a company's financial reports

communicate its economic condition and financial performance during the measurement period. Clinic,2022:51)

2.7 The importance of quality financial reporting

Many studies have indicated the extent of the benefits resulting from the quality of financial reports, including:(Abdul Rahim, 2024: 41)(Gulin al. et 2019)., (Tahir, 2022: 196-197), (Al'Alam, al. et, 2019: 40), (Al-Ajili, 2022: 69)

- Reducing the negative effects resulting from the problem of information asymmetry between management and investors
- Support in making investment decisions as financial reports help investors and creditors make investment decisions.Careful.
- Accurate financial reporting can help reduce poor investment decisions and issues. Ethical, allowing for better identification of investment opportunities.
- Preparing high-quality financial reports is critical to increasing management control and avoiding opportunistic decisions
- The quality of financial reporting plays a vital role in the ability to attract funds. By comparing the quality of the company's financial reports with those of other companies.
- Quality financial reporting results in adequate, transparent, and reliable disclosure of the full results of the business.Activities and operations, which result in providing a true and fair view of performance and financial position.
- Lower cost of capital, higher market value of the company, lower risk of litigation, Improved liquidity levels,
- The positive impact of the high-quality level of financial reports on the financial performance of the company: Improving the quality of financial reports contributes to restoring lost confidence in the financial markets.
- Types and elements of financial reports
- Writers and researchers have divided financial reports into several types, as one of them mentioned that there are: Two types of financial reports: The first type is internal financial reports, which are all financial reports submitted to the various administrative levels in the company. These reports may relate to regular activity or problems facing management. These reports are part of the management accounting system and may be prepared monthly or weekly, depending on what management needs when preparing planning budgets. The second type is external financial reports. This type of report is a means of communication between the company and external users of these reports, such as creditors, current and future investors, various government agencies, banks, and others. These financial reports depict the financial position and performance efficiency of the facility at a specific moment, as in the financial statements that express a previous financial period and aim to meet the information needs of users. The company issuing these reports is obligated to publish the minimum information within the financial reports to meet the users' needs, in addition to other analytical information sourced from the financial statements (Al-Saabri, 2019: 27).

2.8 Factors affecting the quality of financial reports

The quality of financial reports depends on the importance and usefulness of the information contained therein, so several factors available can affect the value of this information, which in turn will affect the quality of financial reports. pointed out(Muhammad, 2022:41) and they are as follows:

1. Material factors include all material components of accounting devices and tools, whether automatic or manual. Which are used to produce information.
2. Human factors include all persons working within the scope of the accounting system and charged with its operation. And provide information through it.
3. Financial factors: These include all funds allocated to operate the system and used to perform its functions and achieve goals
4. Databases contain the application procedures and important data for operating the system, which helps in performing his duties.

2.9 Evaluating the relationship between cybersecurity management and financial reporting

It can For users from evaluation capacity Unity Economic To maintain security Information and avoidance Occurrence of any Breakthroughs The economic unit is exposed to a decrease in the quality of reports, given the decrease in user confidence in the information issued by the unit, which will negatively affect the making of any investment decision and the lack of a clear vision about the future of this unit. Here comes the role of cybersecurity in enhancing confidence for users.

And in Context, Another can study the effect of The report on exposure Unity for attacks Electronic on value Unity And her reputation in Deadline Short And the deadline tall, And that from during Accreditation on style analysis Content damn from 169Companies Included in Stock Exchange Papers Finance American during Period from 2014to 2019, And achieved Unity that it when disclosing Units Economic on Expose it To attack Cyber For the first time It is There is antiquities on Range Short It is represented by in low Returns Daily And more size Trading a result Pressure Operations sale shares Unity Economic, And also There is antiquities on Range tall until five Years It is represented by in Affected Politics Units a result Damages Negativity on value Units And her reputation, where that Breakthroughs Security and attacks Cyber Related In relation Negative with value And reputation Unity As it appears bezel interest Unity Economic By preserving on security Information (Ali and Ali,2022:13).

In addition, it may affect Incidents Security Cyber And the risks The result Lists Finance For economic unity where maybe that Leads to (Abadi, 2023: 69)

- more Expenses Related By investigation And notification By penetration How to treat that And the possibility Litigation And maybe Related to it from Costs Services Legal and others from Services Professional Other.
- low Revenue where It is necessary presentation More Incentives For customers To keep On them and more It is done Their loss.
- low Flows Cash Futuristic or Decay Assets Intellectual or not concrete and others from assets as well as recognition More from Obligations And more Costs Financing).

3. Methodology

This section includes field procedures for research variables. (impact cyber security for companiesCommunications),represented by the data collection method and its interpretation, Conducting a validity and reliability test to ensure its reliability.And its validity, In addition to the study community and sample under which the hypotheses were tested.the study.

3.1 Study community and sample

1. Study community: The study community consists of employees in senior management, audit committees, and internal control in companies. Communications.

2 Study sample: The questionnaire was distributed to a random sample of (90)A category of employees in telecommunications companies, and the results were in Table No. (1) as follows::

ratio	number	Statement	variable
100%	90	Telecommunications companies	**Employer**
77.8%	70	Bachelor's	**Academic achievement**
18.9%	17	Master's	
3.3%	3	PhD	
100%	90	the total	
14.4%	13	Less than 5 years	**Years of experience**
18.9%	17	Between 5-10 years	
36.7%	33	10-15 years	
30%	27	More than 15 years	
100%	90	the total	

4. Study tool

The questionnaire was divided into two parts as follows: The following:

Part One: It consists of demographic data of the study sample and consists of 2 paragraphs.

Part Two: It addresses the impact of cybersecurity risk management on supporting financial stability in companies. Communications, This questionnaire was divided into Two axes.

The researchers relied on the five-point Likert scale to answer the questions. Paragraphs, As shown in the table number (2).

Table (2)Five-point Likert scale

1	2	3	4	5	Degree
I totally disagree	I disagree	neutral	I agree	I agree	**Classification**

3.3: Testing the validity and reliability of the questionnaire

honesty test

The validity of the questionnaire items was verified using the tool method, or what is known as validity. Arbitrators, The questionnaire was presented to the arbitrators, and the researchers responded to the arbitrators' opinions. The necessary measures were taken. Modifications.

Internal consistency validity

The degree to which each questionnaire paragraph aligns with the category to which it pertains for him, Where Cronbach's alpha was chosen (Cronbach Alpha)To prove the validity of the questionnaire for the study and through two axes:

Table (3) Cronbach's alpha internal consistency for measuring the degree of the questionnaire

Axis number	Axis name	Cronbach's alpha Cronbach's Alpha	stability coefficient
the first	Financial stability	0.99	0.99
the second	Cyber Security Risks	0.85	0.91

4.3: Testing the study hypotheses

Several statistical tests were used to analyze the paragraphs. Questionnaire, Extract the arithmetic mean, standard deviation, relative weight, and ranks..

Hypothesis testing for paragraphs: There is a statistically significant effect at the significance level.≥α) (0.05) between cybersecurity risk management and supporting financial stability in telecommunications companies.

Table (4) Support for financial stability

The number	Phrases	Arithmetic mean	Standard deviation	Relative weight	Ranks
1	Cybersecurity risks lead to data breaches that access confidential information about telecom companies' businesses.	3.91	0.85	78.2	3
2	Internal audit provides assurance services on cybersecurity risk management disclosure reports, thus impacting the quality of financial statements.	4	0.088	81.7	2
3	Telecom companies address cyber risks by providing an appropriate cybersecurity environment to support financial stability.	3.74	0.86	75.6	5
4	Telecom companies are overcoming cyber risks resulting from the increasing digitization of financial operations.	4.22	0.88	84.5	1
5	Telecom companies are increasing their focus on enhancing cybersecurity awareness among their employees.	3.82	0.089	76.5	4

6	Telecom companies issue instructions on how to manage cyber risks, and develop policies to manage information security and cyber security.	3.78	0.77	75.5	6
7	"Better integration of cyber risks into financial stability analysis would improve the ability to understand and mitigate system-wide risks" .	4	0.088	80.7	2
Degree		3.78	0.85	71.2	

Table (4) which is shown in paragraph (4) states that telecommunications companies overcome cyber risks resulting from the increasing shift to digitizing financial operations, it came in first place with a percentage of 84.5%, which indicates that telecommunications companies are working to hedge against cyber risks on an ongoing basis, while paragraph (6) which states that telecommunications companies issue instructions on how to manage cyber risks, and set policies to manage information security and cyber security came in last place with a percentage of (75.5%), and since the degree reached (71.2%), it is a high percentage indicating that the IT department includes capabilities or specialists in the field of cyber security and can confront those targeted cyber attacks to support the financial stability of telecommunications companies.

Independent variable: cybersecurity risks

Table (5) Cybersecurity Risks

The number	Phrases	Arithmetic mean	Standard deviation	Relative weight	Ranks
1	Telecom companies are working to address vulnerabilities in the ability of their IT environment to enable their cyber operations.	4.33	0.539	75.1	7
2	Number of reports submitted to senior management by the Risk Management Committee on the number of breaches.	4.31	0.536	77.3	4
3	Telecom companies are developing plans to deal with any cyber risk that threatens their electronic transactions in the future and how to deal with it.	4.32	0.544	78.4	1
4	Disclosure of cybersecurity risks in the report provides relevant information for risk prediction.	4.33	0.541	78.2	2
5	Telecom companies are constantly developing and updating business continuity plans.	3.99	0.498	77.6	4
6	Malware is one of the most widely used techniques for cyber attacks.	4.29	0.511	73.4	7
7	Telecommunications companies prepare and design cyber risk treatments that identify the sources of these risks and the likelihood of their occurrence.	4.10	0.539	74.3	6
Degree		4.23	0.52	76.8	

Table (5) which is shown in paragraph (3) states that telecommunications companies should develop plans to deal with any cyber risk that threatens their electronic transactions in the

future and how to deal with it, it came in first place with a percentage of 78.5%, which indicates that telecommunications companies realize that cyber risks may threaten their electronic transactions in the future, while paragraph (6) which states that malware is one of the most used technologies in achieving cyber attacks came in last place with a percentage of (73.4%), and since the degree reached (76.8%), which is a high percentage, it indicates that there is an expression that clarifies cyber security risks and that the ability of telecommunications companies to confront cyber risks is through providing an appropriate environment for cyber security to support and enhance financial stability.

From the results of the analysis, the researchers conclude that the null hypothesis should be rejected and the alternative hypothesis accepted, i.e., "there is a statistically significant effect at a significance level."($\alpha \geq 0.05$) between cybersecurity risk management and supporting financial stability in telecommunications companies.

5. Conclusions & Recommendations

5.1 Conclusions

- There is a trace ofindicationStatistic at significance level≥α) (0.05 Between risk managementSecurityCyber and supportStabilityFinancial inTelecommunications companies.
- Preparing high-quality financial reports is critical to increasing management control and avoiding opportunistic decisions plays a vital role in the ability to attract money. By comparing the quality of the company's financial reports with those of other companies.
- Cyber security helps to protect the organization's reputation an organization experiences a data breach, it will damage its reputation, and trust between the organization and its customers will be disturbed. Enhancing data management capabilities for most organizations operating in information technology.
- Includes Security Cyber Meanings And implications from Among them Protection and combating, It is also He does on anchoring Criteria from Among them Confrontation Violence And adherence With values and morals And fight crime, Please on foot To practice power from Except for the punishment Legislative And management Organizational in Protection And the confrontation Which They would formation structure Digital Characterized by exactly And control Because it is Depends on Interaction
- Cyber security works on raising the readiness of the infrastructure to confront any possible cyber attacks to be exposed to it suddenly. To protect against cybercrime, which leads to many from Damage and the effects of Negativity on society; where it Depends on the picture President on plagiarism identity The victim in His dealings Finance And Social this affects no Limited Individuals, But it is extend also Organizations And companies,

5.2 Recommendations

- The need to care about security dimensionsCyber by unitsEconomic, especially telecommunications companies, and the pursuit of secrecy in its privacy, Which enhances the company's work and its future.
- Establishing the required physical and human infrastructureDuring training and development of workers is uneconomical to deal with the challenges and problems of cyber security. To benefit from the experiences of developed countries in combating these crimes and benefiting from them.
- The administrations of economic units shall secure their electronic transactions against hacking and electronic piracy, especially since there is a clear expansion in reliance on technology in light of the fourth industrial revolution.KAnd.
- The necessity of raising the capabilities and capacity of departments in telecommunications companies at all their administrative and operational levels. To expand the use of cyber security and improve quality financial reports to contribute to improving the performance of telecommunications companies and protecting their security in light of the security developments taking place at the time.The present.
- The a need to find a strategic action plan that ensures continuity in telecommunications companies and contains procedures stopped due to cyber attacks.
- Attention should be paid to the position. Cyber SecurityAnd his mixture and work are the reason for his passing one of the courses in the diploma, Bachelor, and even higher levels through encouraging graduate students to engage in such a research area.

References

1. Salem,Majedclash,(2022). Iraqi Cybersecurity and its Impact on State Power. Journal of Science Educational and Humanitarian, (18), 69-84.DOI:https://doi.org/10.33193/JEAHS.18.2022.302
2. Adly, Hoda,2021, Cybersecurity Reality and Challenges and its procedures, 2021, magazine Your Law, number16,218-185.
3. Suleiman, Qaftan and Abdel Halim, Bougrine, 2022, Cybersecurity and Related Conceptual ContentsTo him, Tabna Journal of Scientific Studiesacademy, Volume 5, Issue 2.
4. Urethra, generous, 2024, Security cyber, magazineInternational Electronic Research PublishingLegal /Volume4,number18.
5. righteous, Farah Yahya Issa,2022, after cybersecurity Threats to National Security: USA Case Study/ThesisMaster's, university Utah
6. FatherHussein, nostalgic beautiful, 2021, Legal Framework for Cybersecurity Services: A comparison, message's, University of the Middle East
7. M.M. Amna Mohammed Mansour. (2021). The impact of cybersecurity on internal control and its reflection on the economic unit - a survey 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, (127), 223-238.

8. sesame is proven success complete,2022, Politics Cash And its impact on Indicators Stability Financial
via Indicators market head Money, Master's Thesis - University of Karbala.
9. Hamoud, tributaryAbbas, 2023, ImpactCybersecurity on PerformanceOrganization StudyOpinion poll sample of employees in the companyEarthlink,messageMaster's, University of Karbala
10. Al-Saeedi, Khaled Hussein, 2020, effectiveness Politics Finance in investigation Stability Financial in Iraq For the duration(2004-2017)Master's thesis, Al-Qadisiyah University.
11. Al-Asadi, Marwa Ali Ne'meh, 2022, effect Shocks Cash in Stability Financial in Economies SelectedMaster's thesis, University of Karbala
12. Al-Sharifi, Shaima Abdel Hadi, 2022, Relationship between Markets Finance And investment The answer, not Direct And their role in investigation Stability Financial-Experiences Countries Selected with signal, especially For Iraq, Master's Thesis, University of Karbala
13. Othmani, Maryam "Application of e-management in the field of banking services between the necessity of openness and the risks of success." (2019).
14. Al-Medawi, Ali,2023, Cybersecurity Definition - Importance - Types - Strategies to Prevent Cyber Attacks, A Collection of International Studies 34.
15. The shameful, Jahida Saad,2023, Community security contribution to confronting security threats cyber, University of Martyr Hamou Lakhdar in El Oued / University of Mohamed Khider in Biskra.
16. Al-Sumaih, Mona (2020). Requirements for achieving cybersecurity for administrative information systems at the University of King Saud, Journal of the Faculty of Education, Mansoura University, (111) 230-249.
17. God brought it, WalidAbdul Rahim, 2021, Cybersecurity between monopoly and investment,magazineDemocracy, Volume 21, A8.
18. Mohammed, MarwanJasem, 2022, The impact of ownership structure patterns on online discretionary advice and its reflection on the quality of financial reports, a thesis master's,universityTikrit.
19. Clinic, Raghad Abdulcreator, 2022, The impact of the characteristics of the audit committee and the external auditor on the quality of reportsFinance,messageMaster's,universityTikrit.
20. Al-Shammari, Mustafa IbrahimSalman,(2021). Cybersecurity and its impact on Iraqi national security, University of Baghdad, Journal of Legal and Political Sciences.
21. Aqili, Khaled IsmailAbdul Rahim, 2024, The impact of applying generative artificial intelligenceChat GPT "On the quality of financial reports applied to construction and real estate investment companies registered in the stock marketEgyptian, Journal of Financial ResearchAnd commercial, A2.
22. Abdullah, Ahmed, Role Financial Reports in Improving the Efficiency of Financial Markets: An applied study on the Iraqi stock market finance, MagazineScientific research commercial, S11, A1

23. Zureikat, Muhammad Rafiq Muhammad, 2022, The Impact of Cybersecurity Governance on the Effectiveness of Global E-Commerce in Commercial Banks Operating inJordan,messageMasters, University Jerash.
24. Al-Ajili, ImadHamza, 2022, The role of internal audit in evaluating sustainable performance and its impact on the quality of reportsFinance,messageMaster's,universityKarbala.
25. Al-Sabri, Ibrahim AbdelMusa, Mardan, ZaidReturn, 2013, Fair valueAnd the effect of its useIn the quality of reportsFinance, Journal of Accounting StudiesAnd financial, Volume 8, Issue 25 (December 31, 2013), pp. 214-242, 29pp.
26. Gerboua, Adel, 2023, Digital Space and Security cyber, Science MagazineHumanity, Vol. 34, No. 3.
27. Abrahams, T.O., Ewuga, S.K., Kaggwa, S., Uwaoma, P.U., Hassan, A.O., & Dawodu, S.O. (2023). Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security. World Journal of Advanced Research and Reviews, 20(3), 1743-1756.
28. -Seiyaibo, C. M., & Okoye, E. I. (2020). Determinants of financial reporting quality in quoted manufacturing firms: Nigerian evidence. Trends Economics and Management, 14(36).
29. Al'Alam, M. P. A., & Firmansyah, A. (2019). The effect of financial reporting quality, debt maturity, political connection, and corporate governance on investment efficiency: Evidence from Indonesia. International Journal of Innovation, Creativity and Change, 7(6).
30. Gulin, D., Hladika, M., & Valenta, I. (2019). Digitalization and the Challenges for the Accounting Profession. ENTRENOVA-Enterprise Research InNOVAtion, 5(1), 428-437.
31. Sari, L., Adam, M., & Fuadah, L. L. (2024). Determinant Factors of Cyber Security Disclosure: A Systematic Literature Review. KnE Social Sciences, 387-398
32. Docas Akinyele, Simon Daniel, 2024, Building a culture of cybersecurity awareness in the financial sector.