Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

14th International Scientific Conference

"Contemporary insights: Recent developments in the humanities, social and natural sciences"

المؤتمر العلمي الدولي الرابع عشر

"رؤى معاصرة: التطورات الحديثة في العلوم الإنسانية والاجتماعية والطبيعية"

– اسطنبول – تركيا2024 يوليو 15 – 16

http://kmshare.net/isc2024/

The impact of cyber risk management on the strategy for protecting financial assets

Descriptive and analytical research of the opinions of a sample of employees in the Trade Bank of Iraq

Inam Abass Hamidi

Lecturer, Mustansiryah University/Department Internal Control and Audit, Iraq

kifah sami hussein

Mustansiryah University National Center for Hematology Research and Treatment

kifah@uomustansiriyah.edu.iq

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

Abstract:

Today, the global economy has witnessed a new reality characterized by dynamism and rapid change, where the success of any economic unit has become largely dependent on the information it possesses, and the systems and infrastructure connected to networks. Due to the increasing developments in technology and the world of communications, this development has been reflected negatively and in a very large way due to the risks and threats it has created. And hacks and thefts of data and information, which necessitated the development of cyber security strategies and the management of these cyber risks through professional bodies and the development of a framework and guidance guide for companies, especially the banking sector, as it is more vulnerable to risk from time to time, and faces various types of information breaches, which has led to the emergence of real risks resulting from attempts to enter. Unlawful access to data processed and stored in computers, in order to obtain this information for various purposes or attempt to destroy or change it. This emphasizes the importance of cyber security to ensure the protection of the assets of all types of economic units and to protect data and information from hacking and electronic attacks, which constitutes a threat to most of these units in light of Its heavy reliance on electronic data exchange and commercial transactions, which necessitated the need for

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

security guarantees within this digital environment, crystallized mainly in the emergence of cyber security, also known as information security.

Keywords: cyber security, cyber risk management, financial assets, digital threats

Introduction

In light of technological developments and the global world of communications, it was a major reflection of the increase in digital threats through intrusion, cyber-attacks and digital threats to companies and stakeholders (investors, lenders...) and in all sectors, especially on financial assets, especially after the occurrence of the Covid 19 pandemic. This situation has helped increase the ability of information network hackers to achieve high income from cyber security incidents through several programs, the use of encrypted assets, the growth of digital payments, and the increasing reliance and interest by economic units on aspects of technology and information and providers of those services...to address those issues. The increasing attacks and threats to which it is exposed, including professional accounting bodies, have implemented many disclosure requirements with the regulations provided by the AICPA, SEC and others by establishing guidelines and foundations for regulating the process of disclosing cyber risks, and how to manage those risks through developing a cyber-security strategy and protecting the financial

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

assets of the economic unit. Accordingly, the research methodology included:

Study hypotheses: The first hypothesis: There is a statistically significant correlation between cyber risk management and the strategy for protecting financial assets. The second hypothesis: There is an effect between cyber risk management and the strategy for protecting financial assets. Tools and methods: To understand the relationship between cyber risk management and the strategy for protecting financial assets, researchers adopted the descriptive analytical approach, which is widely used by most researchers in the problem of understanding various social phenomena. This method allows realistic analysis of phenomena in order to use the collected data and information to understand the facts, draw conclusions, and identify factors influencing the phenomena to find solutions.

Hypothetical Research Outline: A conceptual study design is created to illustrate the logical relationship between relevant primary or secondary variables. The dimensions of the variables were chosen based on the intellectual capabilities of the researcher, administrative literature, and available resources. The design represents a set of relationships that link the study variables

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

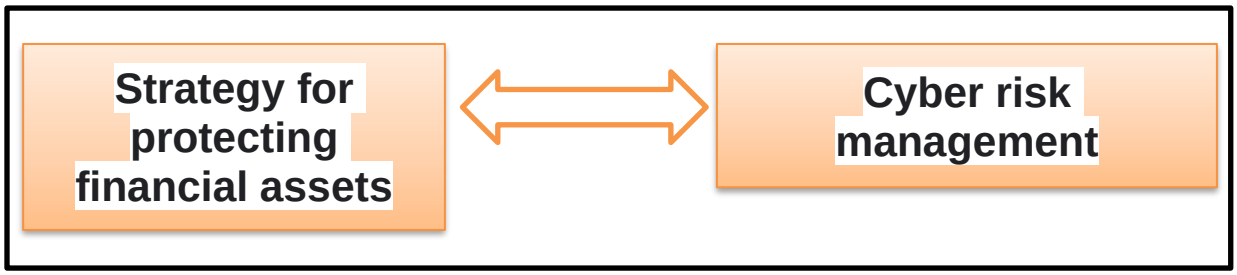


Figure 1: Search Model

Previous studies

1- "How Key Risk Indicators can Sharpen Focus on Emerging Risk" (Beasley, Branson & Hancock, 2010)

"How can the main risk indicators increase the severity of emerging risks?": The study showed that there are many economic units that have adopted an approach to supervising risks through the integrated framework (COSO) of the organization in order to assist the executive management in the process of broadly managing risks.

2- Shafqat N, & Masood A. 2016 "Comparative Analysis Various National Cyber Security"

The study aimed to highlight the weak points in cyber deterrence (cyberspace) and the threats to which economic units are constantly exposed, which leads to a threat to national security, the economy, and the

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

lives of citizens, and to develop a cyber-security strategy to address these threats of all kinds.

3-Cybersecuity Disclosure by the companies on the S&P /TSX 60 Index (Fortin &Herou, 2020) S&P /TSX 60 Disclosure of cyber security in companies according to the Index

This study aims to test the extent of disclosure of cyber risks accompanying the management comments report for companies that include the S&P/TSX 60 index, and these disclosures are consistent with international professional practices in risk disclosure. The research found that companies in all their various sectors disclosed the effects of cyber security risks for the period (2017/2017). 2028), and the research recommended applying stronger standards in financial markets regarding cyber security disclosure.

4- Financial risk management... Strategies for protecting organizational assets...

-https://ar.lpcentre.com/articles/financial-risk-management-organisational-asset-protection-strategies

The article was published on 6/1/2023. Its contents specified how to manage financial risks by protecting the assets that are considered the economic value of the company, through the use of financial tools, and exposing those tools to threats and risks, and managing those risks with the aim of protecting assets or investments in banks. Or business, by

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

enhancing strategic skills about understanding and managing those risks, threats, fraud, and lawsuits. It is necessary to learn how to measure financial risks, analyze financial markets, and protect assets in the economic unit.

The study identified the most important strategies to protect organizational assets from all risks, including the risks of cyber security techniques, before starting to prepare financial reports, following up on performance, and analyzing the results, including: A//-Developing plans in advance to deal with crises, especially cyber security techniques. B//-Classification of critical assets: That is, it is intended to protect assets by classifying confidential information about clients. C//- Using Asset Protection Trusts (APTs) D//- Using insurance E//- Knowing the most effective asset protection tools.

5- Cyber security techniques and risk management in the information age https://ar.lpcentre.com/articles/cyber-security-techniques-managing-risk-in-the-information-age

The article was published on 6/20/2023. The most important divisions of cyber security into several areas, including network security, information security, and application security. It presented the most famous methods of cyber-attack and hacking techniques, including information theft, ransom ware, and social engineering, which is done by clicking on links or downloading malicious applications, which causes... Enabling the attacker

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

to penetrate the computer system and then access the data stored in the calculator. The strategic method is usually used until he clicks to download the application.

Among the most important cyber security technologies are anti-malware programs, access restriction, and DLP technology, which are a technology that provides assistance in making good use of important data when the company's employee makes the mistake of using it poorly, in addition to endpoint security, intrusion prevention systems, and web systems.

6- "FACT SHEET Public Company Cyber security Disclosures; Final Rules" U.S. SECURITIES AND EXCHANGE COMMISSION……https://www.sec.gov/files/33-11216-fact-sheet.pdf

US Securities and Exchange Commission's general final rules for cyber security disclosures

In March 2022, the Securities and Exchange Commission adopted final rules that require disclosure of material cyber security threats and incidents on Form K-8 and periodic disclosure of annual cyber security risks and development of an appropriate strategy for it, through the Commission's proposal for new rules and amendments to the forms and standardization of related disclosures. Material cyber security risks are managed by CO 1934 for companies subject to the Securities Exchange Act's reporting requirements, incidents and threats that pose a continuing and escalating

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

risk to public companies, investors and market participants, and which have increased along with the digitization of registrant operations, the growth of remote work and the ability of criminals. From monetizing cyber security incidents and usage payments.

First: Financial assets

They are intangible assets whose value is derived from a contractual claim, such as bank deposits, bonds, stocks, and participation in corporate capital. Financial assets are usually more liquid than other tangible assets (fixed assets), such as goods or real estate, and whatever the quality of the asset (the asset) is how to protect physical and digital assets from unauthorized access, use, disclosure, disruption, modification or destruction. It includes an application to ensure the confidentiality, safety, and availability of assets in economic units, and its importance and preservation is highlighted as:

1- It plays a major role in generating revenues, managing liquidity, and providing profitable growth opportunities in the long term.

2- Financial data are recorded in the company's balance sheet, and these data are subject to evaluation and reporting standards to ensure transparency, reporting, and financial disclosure.

There are different types of financial assets, including: They are represented in two groups:

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

1- Fixed assets: They are represented by all that the economic units own (furniture / land / machinery /
Equipment/real estate...etc.) (Al-Ani and Al-Yafei, 2016: 233)

2- Current assets, which are:

Stocks: represent ownership in a company and offer potential capital appreciation and dividends.a

Bonds: These represent loans made to governments or companies and provide fixed interest payments and a return on capital.b

C - Cash and its equivalents: includes currency, bank deposits, and short-term investments with high liquidity

Assets are exposed to many financial risks, including credit risks, exchange rate risks, interest rate risks, market risks, liquidity risks...etc. (Most companies are exposed to many risks during the course of their activities, such as the default of some debtors and their inability to pay Their debts to the company, or the decline in foreign currency rates that the company may hold, and the decline in the value of the securities that the company holds for the purpose of investment, or the company is exposed to a financial loss (Abdel Salam, Nadia Al-Sayed, 2022: 497)

Although traded assets are exposed to all of those risks mentioned above, they have increased due to technological developments and the world of communications that have opened new horizons, and at the same time

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

great challenges and new digital threats to their data, represented by theft, hacking, and fraud. These risks can be called (risks). cyber).

Second: Cyber security

The concept of cyber security:

It is defined as “the science that works to provide protection for information from risks that threaten it or attacks from risks that threaten it or attack it, by providing the necessary tools and means to protect information from internal and external risks” (Al-Taher and Al-Khafaf, 2011: 297)

Cook defined it as “the ability to protect or defend cyberspace from electronic attacks, including the ability to detect, evaluate, and exploit potential attacks to confront them through the basic principles of security, confidentiality, and integrity. The practice of cyber security affects national security and economic and personal prosperity.” (Cook 2017:33)

While Edward Amoroso defined it as "means that reduce the risk of attack on software, computers, or networks. These means include tools used to confront piracy, detect and stop viruses, and provide encrypted communications."

Concepts related to cyber security

There are some concepts related to cyber security, including:

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

- Cyberspace: It has been defined by the French Agency for Information Systems Security (ANSSI) as the communication space formed through the global interconnection of automated processing equipment for digital data. It is a modern interactive environment, which includes material and non-material elements, consisting of a group of digital devices and systems. Networks, software, and users, whether operators or users.

"Cyber deterrence: preventing harmful actions against national assets in space and assets that support space operations."

- Cyber attacks: actually undermine the capabilities and functions of a computer network for a national or political purpose, by exploiting a specific weakness that enables the attacker to manipulate the system.

- Cybercrime: a group of illegal acts and actions that take place via electronic equipment, devices, or the Internet, or through which its contents are broadcast.

Political Encyclopedia (https://political-encyclopedia.org/dictionary

One of the causes of cybercrimes

1- The desire to collect and learn information.

2- Seizing and trading information.

3- Conquering the system and proving superiority over the development of technical means.

4- Causing harm to persons or entities.

5- Achieving profits and material gains.

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

6- Threat to national and military security

Cyber security Goals: Goals Security Information

The goals to be achieved by establishing an information security policy are as explained by James. (A, 2004:402) is the safety and security of all processes and sources of the information system and security management can reduce errors, fraud, and losses in the system that connects institutions and stakeholders. Mark (2006:2) confirms that among the requirements for information security is the establishment of a number of laws and regulations. And directives and the level of responsibility for information security to determine the main roles and minimum controls for information security.

Jacques (2008:200) explained that information security requires continuous care and attention in order to track every change to the security of the environment, and this is accomplished through a plan for monitoring, auditing, and acting along the lines of continuous improvement activities that seek to improve information about the state of security over time, and the emergence of new threats. , weaknesses and the effects that arise from them.

Ways to spoof information security

There are many ways to penetrate information security, which leads to unauthorized persons accessing data and information that may be

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

important and confidential. Al-Ta'i classified the methods of penetrating information security (Al-Ta'i, 2004: 156).

1- Competitive Spying:

It means the process of illegal access to the organization's information due to decreased employee loyalty, increased competition intensity, decreased profit margin,

2- Misuse of information:

This is a case in which authorized persons misuse information for the purpose of achieving illegal goals that may be personal or to achieve certain amounts from competitors.

3- Negligence

The main reason for employee negligence is their apathy and weak awareness of the importance of keeping information confidential, or their lack of knowledge of the information that needs protection, and who has the motive to steal it, whether inside or outside the organization.

4- Destruction of information

This process is done by using viruses that destroy programs and information, delete them, distort them, rename them, or change their storage dates.

After reviewing the concepts of cyber security, the departments of economic units in all their sectors must determine how to protect financial

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

assets from digital threats and control them, and what are the procedures followed by accounting and supervisory bodies for these risks.

Here, another role is added to risk management: how to develop a strategy to preserve and protect financial assets from digital threats and cyber risks and how to manage those risks.

Third: Cyber risk management:

Cyber risks are among the most important risks facing most of the company's messages, vision, logo, reputation, or images due to the possibility of unauthorized access or misuse in order to destroy its information (Egyptian Cyber security Authority, 2018: 116).

While the Iraqi National Cyber security Strategy (Cyber security Strategy, 2020, 6)

Define cyber risks (it is the possibility of the existence of a threat and fragility within the country's cyberspace that harms the security of the information system and basic information infrastructure structures through cyber threats and vulnerabilities found in cloud spaces)

Accounting (financial) departments and audit departments in all economic units play a role in managing cyber risks, as they are emerging risks and have significant financial and operational impacts and losses, in addition to

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

the reputation established by managing those risks through cyber security oversight and conducting the necessary tests for the effectiveness of the control elements by selecting... Standard reference points (technology controls) within institutions by emphasizing assurance and advisory services in the areas of information technology.

This is an emphasis on the assurance services provided by auditors, and the effectiveness of the approved programs in managing cybersecurity risks, as well as voluntary or mandatory disclosure in accordance with the evidence and guidelines provided by professional bodies or bodies regulating financial markets... such as the cybersecurity report issued by the Committee Securities exchange on the American Stock Exchange (SEC), and the cybersecurity report of the American Institute of Certified Public Accountants (AICPA) (Kemiyaetal, 2018:3), (Eaton, 2019:2)

Thus, cybersecurity risks are considered among the new risks in the global environment after the Corona epidemic, which required economic units to disclose those risks that they face and that are expected to occur in order to enhance disclosure and transparency in their annual reports (Al-Rashidi, 2019: 466).

Fourth: Accounting professional bodies and cyber risks

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

Due to the increase in cyber threats and risks to the data and information of companies and all sectors, interest has increased on the part of accounting bodies to disclose these risks in the financial markets, especially after the exposure of companies in all sectors, especially the banking sector, as these bodies have proposed a guide and frameworks for identifying cyber security risks and avoiding their effects, which are as follows:

1- The National Strategy for Cybersecurity in Iraq 2018: It was characterized by the national strategy, which is divided into several short-, medium- and long-term strategies and includes a readiness to provide coherent measures and strategic procedures to ensure security.

Protecting the presence in cyberspace, and building and nurturing a reliable Internet community. However, the drawbacks of this strategy are that they include all sectors and do not specify privacy for any sector.

2 - US Securities and Exchange Commission (SEC)

It issued a guideline A in 2018 on cybersecurity disclosure requirements, after it issued a previous guide in 2011 entitled Statement on PROPOSAL mandatory cybersecurity disclosure.

Cybersecurity Goals: Goals Security Information

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

The goals to be achieved by establishing an information security policy are as explained by James. (A, 2004:402) is the safety and security of all processes and sources of the information system and security management can reduce errors, fraud, and losses in the system that connects institutions and stakeholders. Mark (2006:2) confirms that among the requirements for information security is the establishment of a number of laws and regulations. And directives and the level of responsibility for information security to determine the main roles and minimum controls for information security.

Jacques (2008:200) explained that information security requires continuous care and attention in order to track every change to the security of the environment, and this is accomplished through a plan for monitoring, auditing, and acting along the lines of continuous improvement activities that seek to improve information about the state of security over time, and the emergence of new threats. , weaknesses and the effects that arise from them.

Ways to spoof information security

There are many ways to penetrate information security, which leads to unauthorized persons accessing data and information that may be important and confidential. Al-Ta'i classified the methods of penetrating information security (Al-Ta'i, 2004: 156).

1- Competitive Spying:

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

It means the process of illegal access to the organization's information due to decreased employee loyalty, increased competition intensity, decreased profit margin,

2- Misuse of information:

This is a case in which authorized persons misuse information for the purpose of achieving illegal goals that may be personal or to achieve certain amounts from competitors.

3- Negligence

The main reason for employee negligence is their apathy and weak awareness of the importance of keeping information confidential, or their lack of knowledge of the information that needs protection, and who has the motive to steal it, whether inside or outside the organization.

4- Destruction of information

This process is done by using viruses that destroy programs and information, delete them, distort them, rename them, or change their storage dates.

After reviewing the concepts of cybersecurity, the departments of economic units in all their sectors must determine how to protect financial assets from digital threats and control them, and what are the procedures followed by accounting and supervisory bodies for these risks.

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

Here, another role is added to risk management: how to develop a strategy to preserve and protect financial assets from digital threats and cyber risks and how to manage those risks.

Third: Cyber risk management:

Cyber risks are among the most important risks facing most of the company's messages, vision, logo, reputation, or images due to the possibility of unauthorized access or misuse in order to destroy its information (Egyptian Cybersecurity Authority, 2018: 116).

While the Iraqi National Cybersecurity Strategy (Cybersecurity Strategy, 2020, 6)

Define cyber risks (it is the possibility of the existence of a threat and fragility within the country's cyberspace that harms the security of the information system and basic information infrastructure structures through cyber threats and vulnerabilities found in cloud spaces)

Accounting (financial) departments and audit departments in all economic units play a role in managing cyber risks, as they are emerging risks and have significant financial and operational impacts and losses, in addition to the reputation established by managing those risks through cyber security oversight and conducting the necessary tests for the effectiveness of the

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

control elements by selecting... Standard reference points (technology controls) within institutions by emphasizing assurance and advisory services in the areas of information technology.

This is an emphasis on the assurance services provided by auditors, and the effectiveness of the approved programs in managing cybersecurity risks, as well as voluntary or mandatory disclosure in accordance with the evidence and guidelines provided by professional bodies or bodies regulating financial markets... such as the cybersecurity report issued by the Committee Securities exchange on the American Stock Exchange (SEC), and the cybersecurity report of the American Institute of Certified Public Accountants (AICPA) (Kemiyaetal, 2018:3), (Eaton, 2019:2)

Thus, cybersecurity risks are considered among the new risks in the global environment after the Corona epidemic, which required economic units to disclose those risks that they face and that are expected to occur in order to enhance disclosure and transparency in their annual reports (Al-Rashidi, 2019: 466).

Fourth: Accounting professional bodies and cyber risks

Due to the increase in cyber threats and risks to the data and information of companies and all sectors, interest has increased on the part of

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

accounting bodies to disclose these risks in the financial markets, especially after the exposure of companies in all sectors, especially the banking sector, as these bodies have proposed a guide and frameworks for identifying cyber security risks and avoiding their effects, which are as follows:

1- The National Strategy for Cybersecurity in Iraq 2018: It was characterized by the national strategy, which is divided into several short-, medium- and long-term strategies and includes a readiness to provide coherent measures and strategic procedures to ensure security.
Protecting the presence in cyberspace, and building and nurturing a reliable Internet community. However, the drawbacks of this strategy are that they include all sectors and do not specify privacy for any sector.
2 - US Securities and Exchange Commission (SEC)
It issued a guideline A in 2018 on cybersecurity disclosure requirements, after it issued a previous guide in 2011 entitled Statement on PROPOSAL mandatory cybersecurity disclosure.

Fifth: Cybersecurity risks in the banking sector: (Bulletin of the Egyptian Insurance Federation, 2019: 31)

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

The banking sector is exposed to many risks, the most common of which are direct thefts of funds or electronic thefts, which have spread in the name of electronic crimes, in addition to other financial risks such as interest rate risks, exchange rate risks, investment risks, market risks...etc., after the Corona pandemic and the great technological development in The world of communications and technology: Banks have become more vulnerable to digital threats compared to other sectors, such as the insurance sector and the medical centers sector, including:

A - Theft and loss of data / such as personal and commercial data or data of great value to the bank related to black market data.

B - Destruction of data / erasing and encrypting data... and exposure to blackmail, terrorism, or war

T- Theft of money, securities and funds

D - Interruption of communications through disabling e-mail, disabling the network, disrupting the website, etc

Sixth: Procedures followed by the accounting and control departments to manage cyber risks

One of the procedures that must be carried out by the accounting departments or the control and audit departments is to prepare a strategy and it is called (cybersecurity strategy).

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

A cybersecurity strategy can be defined as a high-level plan that helps determine how organizations will secure their assets during the next three to five years. The plan includes a shift from a reactive security approach to a proactive security approach, as the strategy (plan) focuses more on preventing attacks. and cyber incidents rather than responding to them after they occur.

Definition (Delicious/Hassan/2020: 13) is a documented approach to various aspects of cyberspace. It is often developed to meet the cybersecurity of countries and institutions by addressing how to protect data, networks, technical systems, and users of those systems. An effective strategy usually covers all potential attack points that could be targeted by attacking parties.

Delicious/Hassan Hadi M. Basics of a Strong Cybersecurity Strategy/2020

Therefore, the researchers identified the procedures and policies followed by the accounting and control departments in light of the cybersecurity strategy in the form of steps:

A// - (Preparing the internal environment of the economic unit) by setting the most important principles and basic requirements related to cybersecurity for the economic unit in order to maintain it and must be available in the economic unit.

(Al-Aqabi and Al-Rubaie, 2018, 65) identified the most important principles of cybersecurity and electronic data management.

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

Software is based on five principles and their necessary requirements in economic units:

1- Administrative principles and requirements: This includes setting strategies, developing the internal administrative organization, and identifying specialized competencies and skills by senior management in the economic unit.

2- Technical principles and requirements: This principle requires the availability of infrastructure for economic units, including hardware, equipment, and software, which is represented by all the physical components through which electronic applications are implemented via computers, information systems, telephones, and faxes, to provide the appropriate technology for the nature of the economic unit's work.

3- Human principles and requirements: Investment is intellectual capital on which economic units rely through preparing cadres specialized in creating and programming websites, electronic archiving programs, and correspondence through official websites between various economic units, which requires continuous training to keep pace with the rapid movement in the development of the field of technology and communications.

4- Financial principles and requirements: Modern electronic management requires the establishment of specialized training programs and the continuous provision and development of programs. It is considered one of the important and basic principles that hinder electronic management

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

projects and maintaining the security and integrity of information and the economic unit.

5- Security principles and requirements: It requires security and protection of databases and information from internal and external risks to the economic unit, through legislating laws and regulations to ensure the safe access of information to its beneficiaries. (Rashad, Manal, 2022: 6)

2//Means and procedures that achieve information security:

1- Encryption: It is the conversion of writing from its traditional, readable form into secret codes, that is, in the form of unreadable symbols and signs. It is used to ensure the confidentiality, privacy and integrity of the data that is exchanged between different parties in order to ensure that unauthorized parties do not access that data (Al-Tahir, 2010: 104)

Virus protection measures: Viruses are considered one of the most dangerous threats, due to their many types, which exceed thousands. Computer viruses are defined as programs or a set of programming commands that are attached to other programs without the user's knowledge. The effects resulting from viruses are multiple, as the virus may destroy the contents of existing files. On the computer, or erasing some or all of the existing files and data, or it copies itself thousands of times and very quickly, which hinders the work of the system and communications in the network, which requires the use of virus detection

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

programs and attention to updating these programs on a continuous basis to be aware of the latest information.

On new viruses, please do not download or open any file unless the user is confident of its source and do not open any file before testing it (Al-Dawjaji, 2008: 292-293).

2- Preparing backup copies: Backup copies of data and programs are prepared to confront the possibility of loss or corruption of data or programs as a result of operating errors or as a result of the information system being hacked into them.

3- Firewalls: They are a group of interconnected programs located on the borders of the computer network and aim to verify the identity of any person who tries to enter the system, i.e. enter his name and password, as they are matched with the name and password saved in the system's database to determine the persons authorized to access. And access to the system, as well as the possibility of specifying the data that each user can access according to the nature of his tasks and responsibilities within the organization.

4- Password management (password): It is a means whose purpose is to verify the authenticity of the beneficiary, determine the actions that are intended to be performed on the computer, and access the system for the purpose of dealing with programs.

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

There are some considerations that must be taken into account when determining a password, the most important of which are: that the password be long, and that it be changed periodically, that employees' passwords be saved in an encrypted form in the database of the information system, in order to protect against someone accessing and seizing those passwords, And the final connection is cut off from the party who enters the wrong password three times.

3// Protecting financial assets from digital threats...

Protecting financial assets from all types of threats is one of the most important priorities of senior management in the world of digital technology, and the advancement of techniques used by cybercriminals to gain unauthorized access to information and financial assets. From data breaches to phishing attacks and malware infections, the range of threats facing individuals and companies is very wide. They are carried out according to the following steps:

A- Understanding digital threats to financial assets

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

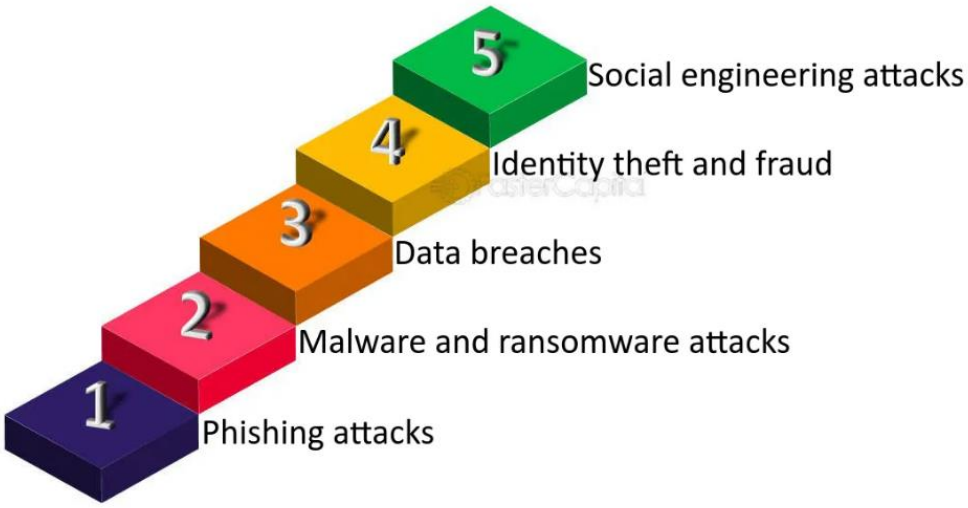


Figure (1) shows the common types of digital threats

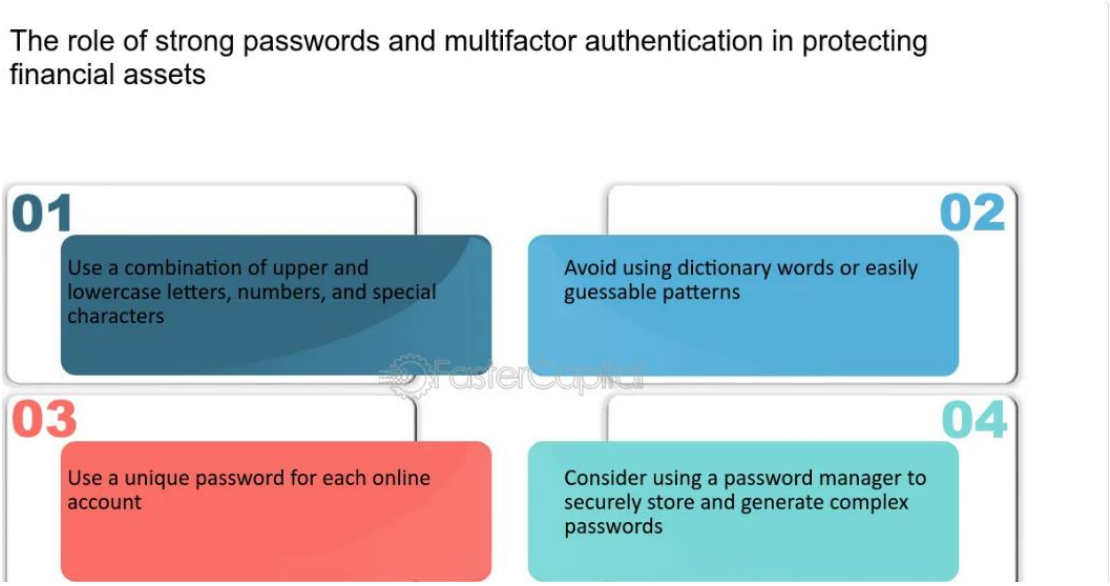
https://fastercapital.com/arabpreneurh Source

B-Realizing the importance of cyber security for financial assets

A single breach can have far-reaching consequences, resulting in financial loss, identity theft, and reputational damage. Realizing the potential impact of digital threats is the key. You deal with sensitive financial data. Power, it is necessary

Figure (2) shows the role of strong passwords and multi-factor authentication in protecting data

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/



3- Security measures to address common types of digital threats targeting financial assets

A- Phishing attacks

Phishing attacks these attacks involve tricking individuals into revealing sensitive information, such as passwords and credit card details, through fraudulent emails, websites or messages. These attacks are often disguised as legitimate entities, such as banks or financial institutions

B- Malware and Ransom ware:

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

Malware and ransomware attacks are malicious attacks designed to gain unauthorized access to computer systems or steal data. Ransomware, a type of malware, encrypts files and demands a ransom for their release.

C- Data breaches:

Data breaches Data breaches occur when unauthorized individuals gain access to sensitive data stored by organizations. These can happen

Breaches are due to insider threats, which are weaknesses in enterprise systems

D- Identity theft and fraud:

Identity theft and fraud Identity theft involves the unauthorized use of information

To someone for fraudulent purposes such as opening credit card loan accounts in the victim's name.

E- Social engineering attacks:

Social engineering attacks include attacks to reveal sensitive information through psychological manipulation and deception due to technical vulnerabilities.

4 //- The role of strong passwords and multi-factor authentication in protecting financial assets

Best practices for protection guidance

You will use a mix of uppercase and lowercase letters, numbers, and special characters.1-

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

. 2-Avoid using dictionary words or patterns that can be easily guessed

3-Use a unique password for each online account.

4- Consider using a password manager to securely store and create complex passwords

https://www.noor-book.com/%D9%83%D8%AA%D8%A7%D8%A)8-The-Basics-of-a-Strong-Cybersecurity-Strategy-pdf

Private or hybrid cloud models and Azure technology

These products allow customers to process sensitive and confidential data in a secure, isolated infrastructure within the multi-tenant public cloud. It also gives the customer full operational control of highly confidential data on-premises, and the intelligent edge capabilities of Azure Stack Hub (formerly Azure Stack) and Azure Stack Edge.

These capabilities process highly sensitive data using a private or hybrid cloud and pursue digital transformation using the cloud for government clients. Key driving factors behind these efforts are enforcing data sovereignty within organizations, addressing custom compliance requirements, and applying the maximum protection available to sensitive data for that sector. By providing Microsoft intelligent data protection technology and intelligent edge approach

Azure

https://learn.microsoft.com/ar-sa/training/modules/design-secure-environment-government/2-discover-cloud-solutions

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

Azure enterprise data protection technology

Protecting sensitive data is essential in the public sector, and Azure technology provides many features and services that protect data throughout the lifecycle of that data. This technology allows government agencies to maintain full control of their data and comply with local regulations around data protection and privacy.

1-Customers use it to meet data protection and privacy requirements for more than 60 global regions around the world.

2- Strong commitments to customers regarding data transfer and residence policies for the customer by limiting Microsoft's deployment area of customer data outside the customer's specified geographic area.

3- Azure provides most services for these services, no storage. Customers can use strong, extensive data encryption options to protect their data, and control who can access it

 How to choose Azure Data Protection in government institutions (public sector)

It consists of the options available to customers to protect their data in technology

1-Customers can choose to store the most sensitive content of their customers in services that store static customer data in geographical locations specified by the customer.

.

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

Customers can further protect their data by encrypting it with their private key using Azure Key Vault 2.
Data encryption during transmission helps protect data from interception

Azure 3 is a service that runs globally 24/7; However, support and troubleshooting rarely require access to customer data

4-Customers who want additional control for support and troubleshooting can use the Customer Lockout box
Azure to approve or deny access to their data.
Microsoft will notify customers of any breach of customer or personal data within 72 hours of the incident being reported
Customers can monitor potential threats and respond to incidents themselves using M6.
https://learn.microsoft.com/ar-sa/training/modules/design-secure-environment-government/3-safeguard-data-azure

The practical aspect of the research
1. Measure variables
Table (1) below represents the arithmetic means and standard deviation for the study variables. The following is an explanation of the table:
1- Cyber risk management variable

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

Table (1) shows the variable of cyber risk management for the Trade Bank of Iraq, where the arithmetic mean of the total variable of cyber risk management was (3.80), which is higher than the value of the hypothesized mean of (3), and with a standard deviation of (.80), which demonstrates the importance of this variable. At the Trade Bank of Iraq level.

2- The strategy for protecting financial assets variable

Table (1) below shows the strategy for protecting financial assets variable for the Trade Bank of Iraq, where the arithmetic mean for the total strategy for protecting financial assets variable reached (3.75), which is higher than the hypothesized mean value of (3), and with a standard deviation of (.77), which demonstrates the importance of this variable to Trade Bank of Iraq level.

Table No. (1) Arithmetic means and standard deviation of the study variables

Table : Descriptive Statistics for Variables		
Variables	Mean	Std. Deviation

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

Cyber risk management variable	3.80	.80
strategy for protecting financial assets	3.75	.77

2. Testing the study hypotheses

The first hypothesis: There is a statistically significant correlation between the cyber risk management and the strategy for protecting financial assets.

The second hypothesis: There is an effect between the cyber risk management in the strategy for protecting financial assets.

A. Testing the first main hypothesis

The correlation matrix table (2) indicates that there is a direct and very strong correlation at a significant level of (0.01%) between the strategy for protecting financial assets and the cyber risk management, It is clear that the existence hypothesis is accepted for the first main hypothesis, which states (there is a statistically significant correlation between the cyber risk management and the strategy for protecting financial assets)

Table No.

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

(2) Correlation matrix

		strategy for protecting financial assets
cyber risk management	Spearman correlation coefficient	.811**
	Sig	.000

B. Testing the second main hypothesis (the effect between the cyber risk management and the strategy for protecting financial assets)

Table (3) shows that the calculated (F) between the total strategy for protecting financial assets variable and the total cyber risk management variable for the Trade Bank of Iraq reached (35.11). This means that there is an impact of the cyber risk management variable on the strategy for protecting financial assets variable for the Trade Bank of Iraq, from here we infer the acceptance of the second main hypothesis. Which states (there is a significant effect of the cyber risk management on achieving strategy for protecting financial assets)

Table No. (3) Impact matrix

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

		strategy for protecting financial assets
cyber risk management	F	32.777
	Sig	.000[b]
	α	.733
	β	.765
	R Square	.733[a]

Discuss the results

a. The results showed that the variable of cyber risk management for the bank in question, which demonstrates the importance of this variable. At the level of the Iraqi Trade Bank.

B. The results showed that the variable of the strategy to protect the financial assets of the bank under investigation, which indicates the importance of this variable at the level of the Iraqi Trade Bank.

C. The research community relied on the research variables, with an average level higher than the variance occurring in the strategy for protecting financial assets. This variance is explained by what the model contains, and (.242) is a variance that is explained by factors that are not included in the model.

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

Dr.. The Iraqi Trade Bank sought to adopt the research variables, with a relatively high arithmetic average, an approximate high interest rate, and reliance on administrative leadership responsible for all directions. Senior management also has an effective role in improving cohesion and reaching the differentiation required to keep the organization always at the forefront.

Conclusions

1. The necessity of the Iraqi Trade Bank strengthening cyber risk management and adhering to it by activating the dimensions of this variable more widely in the bank and opening the way for them to submit new ideas and suggestions or conducting a questionnaire within the Iraqi Trade Bank to know their trends, ideas and suggestions, all in order to enhance the variable. Protecting financial assets in the Trade Bank of Iraq.

2. The Iraqi Trade Bank under investigation should develop a special system for the strategy to protect financial assets through which it can activate its dimensions and train service providers on it.

3. The need for the Iraqi Trade Bank in question to develop the skills level of employees in the Iraqi Trade Bank.

4. Activating the components of cyber risk management by activating its dimensions in a way that achieves and supports the achievement of high levels of sustainable performance.

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

5. Activating the components of protecting financial assets by activating its dimensions in a way that enhances and supports the level of satisfaction and sustainable performance in the Trade Bank of Iraq.

References

First: Foreign sources

1-Cook, Kimberly, (2017),"Effective Cyber Security Strategies for Small Businesses",- Doctor of Business Administration, Widen University

2-James A. Hall, Accounting Information Systems, South-Western Publishing Co., 4th edition, 2004.

3- Ciampa, Mark. (2006): Security + guide to network security fundamentals. Boston: Thomson Course Technology

4- Jacques A. Cazemier; Paul Verbeek and Louk Peter, Information Security Management with ITIL V3, published by Van Haren, 2008.

5-Eaton, T, V, Grenier, J. H. S. Layman D, (2019), "Accounting and cyber security risk management" current issue in Auditing, 13(2), C IC9.

6-Li, Nean G, I, And wang, T, (2018) "SEC S cyber security disclosure, guidance and disclosure cybersecurity risk factors", international journal of accounting information system (pp, 40-55).

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

7- Yang, L, Lau, L, and Jan, H, (2020) Investors, Perceptions of the cyber security risk management reporting framework, international journal of accounting and information management, vol, 28, pp167-183

8 -Beasley, Branson & Hancock, "How Key Risk Indicators Can Sharpen Focus on Emerging Risk," 2010.

9-- Shafqat N, & Masood A. 2016 "Comparative Analysis Various National Cyber Security"

10- Fortin &Herou, "Cybersecuity Disclosure by the Companies on the Inddex S&P /TSX 60", 2020.

Second: Arab sources 1- Al-Taher, Asmahan Majed, Al-Khafaf, Maha Mahdi (2011) Introduction to Management Information Systems, 1st Edition.

Wael Publishing House. Oman. Jordan

2- Alaa Faraj Al-Taher, Information and Knowledge Management, Dar Al-Raya for Publishing and Distribution, Amman, Jordan, 2010.

3-Ali Hussein Al-Dawjaji, the role of the auditor in light of complex information technology and audit risks, Journal of Economic and Administrative Sciences,

4- Al-Taie, Abd Hussein Muhammad Al-Faraj (2004) Advanced Management Information Systems, 1st edition, Dar Wael for Publishing and Distribution. Oman. Jordan

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

5- Al-Aqabi, Nasser Awaid Attiya, Al-Rubaie, Kholoud Hadi Abboud (2018), analysis of electronic management requirements and its role in improving the job performance of human resources

6- Al-Ani: Muawiyah Karim, and Al-Yafei: Fatima bint Hassan bin Saeed, factors determining investment in fixed assets / an applied study from the point of view of managers in a sample of industrial sector companies in Dhofar Governorate - Authority of Oman / Dhofar University, Arab Journal of Management, Volume 36, (December 2, 2016)

7- Abdel Salam, Nadia Al-Sayed, a proposed introduction to reviewing provisions for the impairment of long-term assets, Journal of Financial and Commercial Research, Magazine 23, Fourth Issue, October, Egypt, 2022.

8- Delicious, Hassan Hadi, The basics of a strong cybersecurity strategy, 2020

9- Al-Rashidi: Tariq Abdel Azim, and Al-Sayed Abbas, The impact of disclosing cybersecurity risks in financial reports on stock sources and trading volumes, a comparative study in the information technology sector, Accounting and Auditing Journal, second issue, pp. (439-487).

10- Rashad, Manal Dhaher: The importance of adopting the updated COSO framework and its role in achieving cybersecurity for enterprise risk management in economic units - an exploratory study

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

Third: Articles

1--Egyptian Insurance Federation Bulletin 2019, special issue on cyber attacks, issued by the Arab Insurance Federation, Issue No. 67.

2-National Cybersecurity Authority 2018, Saudi Arabia, pp. (1-40)

3-Iraqi Cyber security Strategy 2019, National Security Advisory, Secretariat of the Supreme Technical Committee for Communications and Information Security, pp. (1-15)

4- Cybersecurity in Iraq: A reading of the Global Cybersecurity Index, 2020, Al Bayan Center publications

For studies and planning Iraq.

5-Ali, Mahmoud Ahmed, and Ali Saleh, the impact of disclosing the cybersecurity risk management report on the investment decision

In the shares of companies listed on the Egyptian Stock Exchange: An experimental study, the Fifth Scientific Conference of the Accounting and Auditing Department

(Challenges and Prospects of the Accounting and Auditing Profession in the Twenty-First Century) for the period (10-11), 2022.

Fourth: Internet sites

7-https://fastercapital.com/arabpreneurh

Global Proceedings Repository
American Research Foundation
ISSN 2476-017X
Available online at http://proceedings.sriweb.org
شبكة المؤتمرات العربية
http://arab.kmshare.net/

8-https://www.noor-book.com/%D9%83%D8%AA%D8%A7%D8%A)8-The-Basics-of-a-Strong-Cybersecurity-Strategy-pdf

9-https://learn.microsoft.com/ar-sa/training/modules/design-secure-environment-government/2-discover-cloud-solutions

10-https://learn.microsoft.com/ar-sa/training/modules/design-secure-environment-government/3-safeguard-data-azure

11- https://political-encyclopedia.org/dictionary

12--https://ar.lpcentre.com/articles/financial-risk-management-organisational-asset-protection-strategies

13- https://ar.lpcentre.com/articles/cyber-security-techniques-managing-risk-in-the-information-age

14--" FACT SHEET Public Company Cybersecurity Disclosures; Final Rules" U.S. SECURITIES AND EXCHANGE COMMISSION……https://www.sec.gov/files/33-11216-fact-sheet.pdf