ROLE OF CYBER SECURITY ABOUT IMPROVING OF DECISIONS OF STRATEGIC FINANCIAL: AN EXPLORATORY STUDY OF UNIVERSITIES OF IRAQ

Rahman Zghair Hussein*, Mohammed Safaa Salman

Faculty of Administration and Economics, Misan University, Amarah, Maysan Governorate, Iraq.
*Corresponding author, email: rahman.z.h@uomisan.edu.iq

doi: 10.17977/um066.v6.i7.2026.4

Keywords

Cybersecurity
Information systems
Digital infrastructure
Cyber awareness
Quality of financial information systems
Strategic financial administrative decisions

Abstract

The main objective of this study is to examine the impact of the technical, organizational and human elements of cyber security on the capacity of financial management in Iraqi universities to make sound and reliable financial decisions. Digital systems use in financial and administrative methods, particularly. The two researchers found that the Iraqi universities have experienced an unprecedented growth. Therefore, this research aims to concentrate the growing concern of university management in information security, particularly in the current international and local environment of growing cyberattacks and data manipulation, which can have a negative effect on the credibility and clarity of financial statements and on the sustainability of investment plans. The two researchers also shared with the relevant parties and compared among the universities the differences related to digital infrastructure and the availability of qualified staff. The disparities directly affect the robustness or susceptibility of cybersecurity frameworks and information security strategies. The research method was descriptive-analytical, and the most important tools used in it were the questionnaire which included 120 forms distributed to a sample of students consisting of administrative and financial employees, faculty members from different public and private Iraqi universities. The aim was to gather field data that would add to obtaining accurate scientific outcomes. The statistical analysis showed that the reliability coefficient obtained for all the research variables was 0.767 and the validity coefficient was 0.876. These values signal a strong degree of internal consistency and verify the suitability of the study variables for next statistical analyses. Furthermore, the results showed that all the main research variables had a significant and strong correlation (0.05), and all were important. Data were also analyzed using a number of appropriate statistical methods and tested with the hypotheses of the study.

1. Introduction

Confidentiality, Integrity, Availability (CIA) principles are crucial to the overall cybersecurity mission, as they form the backbone of data security when it comes to strategic financial administrative decision making based on accurate and secure data. Given the significant growth of data processed and the complexity of financial and administrative procedures in universities, the need for a secure environment, where technical, organisational and human factors cooperate, has become more apparent than ever (Cram et al., 2019).

In recent years, universities have become increasingly based on information and communication technologies to administer their activities. Thus, the basic tools for processing, storing, and exchanging information are computer networks and the Internet. That's why these networks require strong security policies to protect their content and maintain their management. Moreover, public and private universities became more crucial in web technologies and electronic financial management mechanisms, making them more vulnerable to cyberattacks, which are one of

the most significant threats that higher education institutions should be able to cope effectively with (Amir et al., 2018).

Among the most severe threats that universities and other institutions face are cybersecurity intrusions that affect the trust of all stakeholders in the investment and operating process, including students, investors, customers and everyone else. The loss of trust does not just apply to the institutions that are directly impacted by cyber incidents and cyber breaches, but it can also extend to other organisations in the same industry sector. Moreover, cybersecurity risks are acknowledged as among one of the most major challenges to global economy's stability and development. Institutions, be they educational or not, may suffer significant economic and financial losses as well as be harmed in their standing and reputation from cyberattacks. These adverse effects often extend outside the targeted institution to impact the whole industry, a phenomenon common mentioned as the "contagion effect" (World Economic Forum, 2017; Kamiya et al., 2018; Kelton, 2019).

Due to the growing dependence on virtual administrative operations, the rapid expansion of the Internet and the rise of big data governance, many organizations require senior management to have a complete understanding of their vulnerability to cyber threats and how they can use such threats to assist in their strategic financial management decisions (Bozkus Kahyaoglu & Caliyurt, 2018).

Moreover, the ubiquity of the changes in communication technology has given rise to a great deal of observation and monitoring practices that have not only targeted institutions but also people. The use of electronic communications and the social media network has become commonplace, and there are examples of both individual and well-coordinated attempts to use cyber means for various cyber activities, including threats to electronic communications and social media networks. This has left personal confidentiality and sensitive information open to the risk of unauthorized access, and resulted in an increase in incidents such as cyber blackmail, electronic fraud and other forms of cybercrime. Therefore, there is no way, neither an individual nor an organization, can be shielded from cyberattacks aimed at unauthorized access, theft of data and misuse of digital resources (Richardson et al., 2019).

Today, data and information are strategic assets for organizations, especially in the context of the fast-paced digital transformation currently underway in Higher Education Institutions. As a result, cybersecurity has emerged as a key element to ensuring these data's protection and to financial management's capacity to make secure, strategic, and correct decisions. The reliability of accounting and financial information systems are today regarded as one of the most critical issues in today's organizations and Cyber threats are one of them. This then can have a negative impact on managerial decision making systems (Alshaikh et al., 2020; Ahmad et al., 2014).

With the increasing awareness paid to the importance of cybersecurity in educational institutions, studies that investigate the direct impact of cybersecurity on the quality of financial management decisions are still scarce, especially in the Iraqi context. There are many challenges in Iraq for the technological infrastructure, human resources and organizational culture of the information security issue in universities. Therefore, this study aims to explore the impact of cybersecurity components - namely technical, organizational, and human items - on supporting strategic financial administrative decisions in Iraqi universities. For this purpose, a descriptive-analytical approach was employed, focusing on the field data obtained from administrative and financial staff (Ab Abbas & Shaker 2022).

The sector of financial administration has gone by way of appreciable changes lately. Initially, financial management was primarily focused on the acquisition of the resources to conduct the processes of the organization. But modern literature has widened its scope much to include optimizing the allocation and use of financial resources, making financial and administrative decisions, and managing financial risks (Siti, 2023).

Economic institutions have acknowledged a significant role in the writings and studies of early economists, because they are interested in the core of the economic activity of a society. But social units are also considered institutions because of the relation between the human resources with the material and intangible resources in the way of operation of the institutions. There are different types

of organisations such as service organisation, agricultural organisation, industrial organisation, and commercial organisation, and all try to be profitable and sustain the organisation.

One of the main goals of an organisation is to produce profit. The institutions need to depend on their core functions and coordinate the various functions appropriately in order to perform their functions successfully and to reach the planned objective. These functions vary from institution to institution and depend on the nature, objectives, and activities of the institution. However, some functions are shared by almost all organizations and both financial management and human resource management are important for improving organizational performance and fulfilling strategic goals (Yassin et al., 2024).

Most importantly, universities function in a context of constant changes and volatility, and therefore, it is important to closely monitor the financial management system that will enable their sustainability and long-term viability. There must be sufficient financial and administrative resources available in universities to repair their operation to meet their strategic goals. Therefore, the functions of financial management are closely related to the growth and development of universities and their activities in an effort to bring about the liquidity required to support the objectives of the university.

Financial management also involves linking up the efforts of various parties within the university to create performance, utilize available resources effectively and ensure the availability of financial resources. It primarily focuses on defining the need for funding and resources, ensuring that the right funding is obtained at the right time, identifying resources for funding and ensuring that financial resources are used effectively. Hence, the importance of financial management has a significant impact in making an institution more capable of answering the challenge and dealing successfully with crisis.

1.1. Research Problem

The ever-changing dynamics of the business scene have led a number of organizations to quickly embrace modern applications of technology and digital tools in their operations to increase efficiency and effectiveness. Also, most universities increasingly depend on electronic networks for storing and managing their critical data and information. Meanwhile, the nature of the global business environment demands that organisations keep their infrastructures secure and provide digital means to conduct their operational and financial payments efficiently.

This interconnected global digital infrastructure is often cited as cyberspace, consisting of the Internet, computer systems, applications of programs and digital information resources. With the increasing reliance on cyberspace, protecting such digital assets from cyber threats and security breaches is increasingly becoming a significant focus in ensuring business continuity, protecting sensitive information, and facilitating effective organizational decision-making (Bozkus Kahyaoglu & Caliyurt, 2018).

As digital financial and administrative services have evolved, the number of cyberattacks has increased by a factor of more than double in the past 10 years. Financial and administrative systems are still among the most commonly targeted areas by cyber attacks, despite their progress in testing new cybersecurity measures. As such, cyberattacks have emerged as an integral part of the financial stability and organizational productivity threats.

In addition, the economy's rapid digitalization and reliance on institutions for information technology systems have put cybersecurity at the top of the organizations' risks agendas. Knowing how much cyber risk is present in universities with the financial-administrative and technological perspectives is key in this context. Such understanding enables institutions to better prepare for potential cyberattacks, reduce their results, and reduce the financial losses related to cybersecurity incidents.

In the last few years, Iraqi universities have been gradually relying on electronic systems and internet services through various services that are inherent in their educational process, such as the financial administration and student affairs, etc. This digital shift has not only enhanced the efficiency

of university operations, but it has also increased the universities' exposure to cyber threats which could impact the safeguarding of financial data and integrity of administrative decision-making.

Academic and government bodies in Iraq, in response, have embarked on initiatives aimed at bolstering the cybersecurity awareness and capabilities, which include arranging specialized forums, training programs, and initiatives to boost digital infrastructure. In addition, there has been a focus on cultivating skilled personnel who can ensure a balanced approach between digital progress and cybersecurity needs.

However, this research is limited in scope to examining the relationship between cybersecurity and its implications for strategic financial management decisions in the local university context, with the relative lack of research in this area. Specifically, there has been limited research to assess the success of cybersecurity policies and procedures, and the readiness of university administration to respond to cyber incidents that could impact financial decision-making processes (Khalid et al., 2022).

An incident related to cybersecurity, or a cyber threat, can cause immediate financial and administrative harm due to the loss of assets, sensitive data or the disruption of financial operations. Apart from these direct impacts, the institutions can also suffer from serious indirect impacts like loss of trust among the stakeholders and students, and also harm to academic reputation and institutional credibility.

Thus, the better the cybersecurity practices that are carried out in universities, the lower the risk of cyber incidents and the less negative economic and administrative impact they have. Empirical evidence suggests that significant cyber security incidents or breaches can cause significant and enduring losses in institutional value, financial performance and organizational effectiveness. The results underscore the need to develop effective Cybersecurity institutional structures to protect the operation of Universities and facilitate sustainable strategic decision making (Sharma et al., 2023).

From the discussion above, the following research questions can be stated in regard to the research problem: 1) What's the concept of cyber security and what are the risks involved with it? 2) What does financial management do for the administration of strategic decision making? 3) What is the impact of technological progress on the objectives and activities of financial management? 3) How big are cyber security problems and threats in the financial management of universities? 4) What is the influence of cybersecurity on supporting strategic financial management decisions in Iraqi universities?

1.2. Research Objectives

The aim of this research is to test and analyze the effect of cyber security and the necessary elements and factors that play a significant role in supporting strategic financial choices in Iraqi universities. The study also looks into the major challenges and obstacles that prevent the fulfillment of the cybersecurity requirements, and the effects that result from the challenges.

More specifically, the research is to solve the research problem through the following research objectives: 1) To understand the concept of cybersecurity and understand the threats and dangers of cyber threats. 2) To demonstrate financial management's part in strategic decision making support of administration. 3) To explore the effect of technological advancements on functions and practices of financial management. 4) To recognize the financial management related cybersecurity issues & threats prevailing in the universities. 5) To measure the effect of cyber security on promoting strategic financial management solutions in the Iraqi Universities.

1.3. Research Importance

1.3.1. Academic Importance

Recent years have seen an escalating rise in the importance of cybersecurity, especially in the context of helping to inform strategic financial management decisions. As a result, the importance of information provided by universities has greatly increased, as this information is a major source of information for strategic decision-making. In addition, there is an expectation that cybersecurity

information will be comprehensible, comparable and provide adequate and meaningful information to stakeholders and decision makers. The academic importance of this study is reflected in the following points:

The study responds to the lack of studies in the academic literature on the linkage between cybersecurity and how it is used to support strategic financial management decision making in the context of higher education institutions within the Iraqi University context where studies on this subject are limited.

The study focuses on the role of the components of cybersecurity – technical, organizational and human factors in improving the quality of strategic financial management decisions, thereby laying the groundwork for further studies in this area by researchers.

The study helps build and strengthen conceptual frameworks and principles on the significance of cybersecurity in administrative and financial decision-making processes in alignment with the current global trends and best practices.

1.3.2. Practical Importance

In recent years, with the ongoing digitization of business activities, cybersecurity has become one of the most relevant areas that is attracting a lot of attention both nationally and internationally. The changing landscape has led to more cyber threats and the increased risk of data breaches, which is why cybersecurity risk management is a key focus for organizations. As a result, more organizations are being urged to make it abundantly clear how they identify, evaluate, and reduce cyber risk, with the attention regulatory bodies and specialized committees give to this topic increasing.

An effective application of cybersecurity management methods and the adequate mitigation of cybersecurity risks can greatly enhance an organization's capability to respond to technological and cybercrises. This can be done by detecting and closing security gaps, filling gaps in information structures, fortifying information security policies, and helping with administrative and financial security. This study is of practical significance because of the following: 1) To help university administrators implement more effective cybersecurity policies and procedures to protect financial data and enable accurate financial administrative decision making to enhance the effectiveness of Iraqi Universities. 2) To help minimize errors and risks related to cyberattacks or vulnerabilities in security systems and thus increase the stability of strategic financial administration decisions and associated risks. 3) To support strategic planning of Iraqi universities towards satisfying the needs of the digital environment for better adaptation in order to gain and enhance competitive advantage in the higher education sector.

Improve the capacity of financial and financial administration planning officials in universities through making practical recommendations based on the results of the study, which can be put in practice to better the quality of the financial planning and benefit the decision-makers.

1.4. Theoretical Framework

1.4.1. What is Cybersecurity?

Cybersecurity means the defence of users and assets from any threat in the online space. However, the meaning of cyber security in the present time has expanded from being an issue of insecurity to a substantial issue that needs serious care and the adoption of adequate measures to protect the internet users. Today, along with the technical issues, there are different social challenges where Cyber security comes into play.

In this respect, cyber security is the group of processes and resources that ensure that the cyberspace and all systems that are connected to it are safe from illegal incidents and activities that are in violation of the legal regulations. It includes every measure designed to safeguard digital environments, and ensure integrity, confidentiality, and availability of information systems (Al Shamsi, 2019).

It is an activity which guarantees the protection of human and monetary resources linked to information and communication technologies. It also gives assets the ability to reduce losses and damages that could occur due to risks and threats. Furthermore, it helps to restore normal circumstances quickly, which prevents the interruption of production processes, and consequently reduces damage into permanent loss (Al-Baghdadi, 2021).

It refers to a set of conditions or events related to enhancing the security of the information management system or the relevant infrastructure, as well as addressing current and emerging challenges associated with this area. It is a term commonly used to refer to all actions undertaken to keep information technology resources secure. It also involves the gathering and structuring of resources and personnel and processes to be able to preemptively prevent threats, identify those threats, isolate them and solve them, both in order to ensure the continuity and integrity of the information technology framework (Schiliro, 2022).

From the above, the researchers deduce that, Cybersecurity: Set of policies, procedures, and technologies designed to protect information systems and digital data from both internal and external threats. Cyber security is more than just technological aspects, it also involves risk management, human awareness building and organizational arrangement improvement.

Its core aim is to protect digital assets from sophisticated and constantly changing threats, while also ensuring business continuity and the integrity and security of information in today's fast-paced digital landscape.

1.4.2. What is Cybersecurity Risk?

Cybersecurity risk is a series of technological, operational and organizational risks that are encountered by companies using modern information technology systems. These risks can come from violations of cyber systems, which can impede the organization's ability to achieve its goals (Perols & Murthy, 2021; Florakis et al., 2020; Badawy, 2021; Hartmann & Carmenate, 2021).

Cybersecurity risk can be defined as the process involved in identifying, analyzing, and evaluating cybersecurity risks, then developing strategies and techniques to lower the risks, but not to an unacceptable level, while maintaining continuous protection in line with the ever-changing nature of the cyber risks (Al-Ajlan, 2024).

Security vulnerabilities, from the researchers' perspective, are potential threats to information systems, digital data or technological infrastructure, and which can lead to loss of data, leakage of sensitive data, disruption of services, reputational damage, and financial and operational loss. These risks generally include three elements: threats, vulnerabilities and impact.

1.4.3. Objectives of Cybersecurity

The goals of cybersecurity can be described as follows (Haapamäki and Sihvonen, 2019). Cybersecurity is about the security of confidentiality of private and sensitive information. It ensures that authorized users can gain access to information at the appropriate time when necessary, and cybersecurity helps to protect the accuracy, consistency and reliability of information. Based on the aforementioned, the researchers summarize the goals of cybersecurity as follows: protection of information confidentiality, which means secure the sensitive data so that it cannot be accessed by unauthorized or malicious users; data integrity, which means ensuring that all data is maintained in such a way that no unauthorized changes (modification, deletion or manipulation) are made to it; system and service availability, which means guaranteeing the availability of information resources to users at all times so as to support the accuracy and continuity of their access; cyber risk management, which refers to the process of identifying internal and external risks, threats, opportunities, strengths and weaknesses and then developing strategies to reduce potential risks; and development of a secure digital environment, which refers to creation of trust in the electronic systems among the stakeholders in supporting the accurate and timely decision making processes.

1.4.4. Cybersecurity Risks

Some of the types of cyber risks are as follows (Shahimi, 2018):

Confidentiality-related cyber risks

These risks are encountered when there is a release of confidential organization information to third parties, such as in the event of a breach of information. Integrity-related cyber risks: These risks include misuse or manipulation of systems, including fraud or unauthorized changes to information. Availability related cyber risks: These are risks to the availability or interruptions of business activity that could lead to a failure in maintaining normal organizational operations and/or service continuity. There are two types of cybersecurity threats, namely (Li et al., 2019; Perols & Murthy, 2021; Badawy, 2021; Hartmann & Carmenate, 2021; Farag et al., 2017). Performance related cybersecurity risks: These are related to the use of modern information technology tools and relate to the inability of these tools and their use to perform the required functions or to achieve the intended benefits and objectives.

Security Risk Group

The security risk group includes three main types of risks, as follows:1) **Physical Security Breaches** are unauthorized access or intrusion into the physical components of an organization's information technology infrastructure. These components provide information technology services for the organization and can be hardware, storage media, and network devices. A typical form of such violations is dumpster diving, the practice of rummaging through an organization's junk—floppy discs, networking devices and the like—to obtain confidential data. Data, documents or passwords that may be found on these discarded items can be used to enable unauthorized access or to finalize a cyber intrusion. 2) **Eavesdropping on Emanations** is the process of capturing and intercepting all wireless or electromagnetic emissions of an information technology system, using specialized devices. These can be in the form of audio waves or other means of electronic leakage that can be used to obtain sensitive information from the system without having to physically access it. 3) **Personnel security breaches** are connected to internal and external risks that are linked to an employee's behavior in an organization. Software piracy, in which software programs are copied or used without authorization, and authorization violations due to inadequate internal control systems are some of these risks. They also feature social engineering attacks, where the employee is tricked or coerced into accessing confidential information via work connections. Also, session hijacking is the unauthorized access or takeover of an active communication session to access private information or systems.

We have not yet seen any breaches of communications and information security. There have been no communications and information security breaches seen so far.

Communications and information security breaches are incidents that target data and communications systems used in an organization. This includes data attacks like unauthorized copying of data, where sensitive data is illegally duplicated or extracted. These also involve software-based attacks, such as the presence of malicious software (viruses, traps, backdoors) to compromise the security of information systems, and for this purpose. Covert channels are also implicitly established communication pathways that allow the transfer of information that circumvents explicit security channels and monitoring measures.

1.4.5. The concept of strategic financial management.

Strategic Financial Management Concept Oqaili (2014) conducted a study on the definitions of SFM and he summarized a number of the definitions as follows:

Financial management is the managerial activity focused on the creation and maintenance of economic value or wealth by effectively managing and utilizing financial resources and implementing decisions that add value to the organization and increase its value, according to Keown et al.

According to Grape and Brigham, "financial management is the managerial activity that involves financial planning, the acquisition of financial resources, and the effective use of financial resources to maximize the effectiveness of an organization's operations and achievements. In this view, the goal

of financial management is to maximize the efficiency and effectiveness of financial planning and use of resources. This definition aligns with the classical school of financial management which considers "financial management" as the process of fund raising, control and management of funds to ensure that the objectives of the organization are realized.

Financial management, according to Howard and Upton is the administrative area, or set of managerial activities, that focuses on the management of cash flows in ways that allow the organization to accomplish its goals efficiently and effectively and pay its bills when they are due. This definition highlights the role of effective cash management as a key enabler to continuity and the success of the strategic objectives of an organization.

Financial management refers to the process which has a significant contribution in financial planning, asset management and solving unusual issues that may arise in the company to maintain the continuity of the company and to be able to realize the objectives of the company, Johnson said. It also includes the provision of sufficient liquidity and financial facilities to ensure the availability of funds to fulfill their financial commitments when they become due.

Financial management is also regarded as the set of managerial functions and activities related to the coordination and management of the financial needs necessary to the efficient and effective accomplishment of the project's targets. It aims to manage financial resources better and make the most of them, improve performance and productivity, and pay financial duties on time.

By the above definitions, the researchers were able to deduce that strategic financial management is the holistic approach to financial planning and management which serves to meet organizations needs of resources, namely assets and liabilities, needed to realize success and continuity. Strategic financial management is not just about cash flows or budgeting; it is a holistic managerial approach that is connected with investment, financing and operational decisions and is linked to the strategic goals of the organization. This is done to gain a sustainable competitive advantage and to maximize the value and shareholder returns of the organization in the long run, by efficient use of financial resources and effective risk management.

1.4.6. Functions of Strategic Financial Management

The literature on strategic financial management has outlined a number of key functions, most notably the following:

Financial Forecasting and Planning: The financial management coordinates the activities of financial planning and forecasting in the organization. This involves coordination and collaboration with other organizational units/areas in order to optimize efforts and accomplish organizational goals. Financial planning: Activities involved in examining the financial performance of the organization over the past, analyzing the financial situation of the organization, and forecasting its future financial needs. Financial forecasting, however, is the science and art of predicting the future of financial events and conditions to aid financial and strategic decision making.

Successful organizations experience a steady growth in sales and generally require additional investments in machinery, equipment and technologies to be able to meet the rising demand for their products and services. In this case, financial management is a vital component of investment and financing decisions by determining assets and projects that have to be invested in and choosing the most suitable financing options for investment in assets to achieve goals and improve financial efficiency.

Coordination and Control: Financial Management staffs have to coordinate with employees of other departments on all decisions made within the organization. All decisions that are made have an actual financial impact.

Risk Management: The organization is subject to many risks that are systematic, meaning that they impact the environment in which the organization operates, for example, inflation, economic growth, economic recession, wars, and political instability. It could also have threats that do not

impact other organizations but do affect the organization itself, for example, the failure to market the products. Hence, the financial analyst should take intervention.

The researchers found that the goals of strategic financial management can be represented as: Value maximization of the organization, balancing risks and returns, financial efficiency, contribution to sustainable growth, financial stability, ensuring correspondence of financial goals with overall strategic goals, and providing accurate financial information for decision making.

1.4.7. Characteristics of Strategic Financial Management

Financial management is part and parcel of the administration of the university as a whole and the salient features of financial management are as follows: 1) It infuses every facet of education; no activity is treated without financial issues. 2) Universities often have to make financial decisions that have an impact that extends well beyond the immediate scope; hence, great care must be taken with financial decisions.

There are some financial administrative decisions that can make or break the success of the educational system, and are critical to universities.

The researchers find that there are several attributes of strategic financial management that make it a valuable instrument to pursue long-term goals of universities. These are the most relevant: Sustainability and long-term profitability, integration into the overall university strategy, future-oriented approach and risk forecasting, adaptation to economic, financial and technological changes, risk management (taking appropriate precautions) and the use of information and financial analysis to process and analyze data. The objectives of Strategic Financial Management are:

Profit maximization Objective: Profit maximization is very close to with investors and are a key part to assessing the efficiency of management activities. Profit maximization is an objective, which is followed by capital owners, and becomes the first guiding principle of financial management in making financial decisions. The effectiveness of the financial department or financial function is also assessed in terms of how it enables them to meet this objective. There is a difference between profit, which represents a share received by investors either directly as distributed net profit or indirectly as retained earnings, and profitability, which refers to the ability to obtain greater economic results from the resources utilized.

The profit maximization objective does not consider some fundamental and important factors such as expected return, timing of return and risks involved in return. Furthermore, it is not enough to meet the goals and interests of everyone who is involved in the firm's operations. This resulted in the development of an objective that considers the timing and benefits of returns, and the quality of the benefits obtained. This is reflected in the objective of firm value maximization which means maximization of the value of shares of the firm in the securities market.

Social responsibility is one of the problems that face the identification of objectives related to financial management, this is called social return maximization objective. The institution considers the effects of its policies and activities on all the elements of the society in which it functions and hence has a prominent role to serve the community.

1.4.8. The function of financial management in strategic decision making process

The decision-making process in an organization can differ on several bases. The decisions are taken on the basis of time criterion are long term and short term decisions, on the basis of importance criterion, strategic and tactical decisions, on the basis of functional criterion there are several types of decisions, the most important of which is financial decision. A financial decision, on the other hand, is a managerial decision that must be made to address a specific situation and plays a vital role in the study of financial management. A strategic financial decision can be defined as “the determination or selection of one of several possible or alternative solutions to achieve a specific objective or address a particular situation related to the financial and administrative aspects of the organization’s operations, and which has a significant impact on the organization’s liquidity and future” (Zahwaniet al., 2017).

Financial decision making involves all administrative aspects such as financial planning, organization and control. The role of financial planning, especially the strategic components of financial planning, in financial decision-making are quite significant because it shows the implications of financial decisions in the long term. Additionally, the efficiency and capacity of an institution or responsible authority to make sensible and effective financial decisions is heavily reliant on its proficiency in understanding the financial environment, analyzing strengths and weaknesses, exploiting opportunities, mitigating threats and reducing negative impacts of financial environmental factors on financial decisions.

The researchers found that financial management is a key part of the strategic decision making process in Universities by: providing financial information which can assist decision makers in determining the most appropriate strategic alternatives; evaluating strategic alternatives by analyzing the financial impact of strategies such as expansion, investment, mergers or acquisitions; long-term financial planning for support and to enable evaluation of strategies and identification of financial needs; financial risk management; efficient allocation of resources to achieve financial return; and performance monitoring, analysis of deviations and periodic reporting to support evaluation and adjustment of strategic alternatives.

1.4.9. Strategic Financial Decisions:

Some of the decisions that are made are part of the Strategic financial decision making, including:

Strategic Goal of Financial Decision Making

The goal of an organization in making financing decisions is to maximize the wealth of the investors through maximizing the value of the firm which is measured by the market value of the common shares of the firm. Thus, the management has to decide how it is best to raise the amount needed with minimum cost.

The rules governing the financing process comprise several principles that regulate the financing selection process and limitations required to make the right financing mix. There are several rules that apply to this process:

Minimum Financial Balance Rule

This rule is about the financing of fixed assets with permanent financial resources. Investments can be funded from medium or long-term debt, self-financing or equity funds, for instance. Operating assets should be financed with operating resources, e.g. supplier credit, and the like. Not following this rule during financing could result in a number of issues, primarily in the area of getting an urgent cash flow need and a dramatic drop in working capital.

Financial Independence: to borrow no more than you can afford at any given moment. So, for any given individual, the financial independence factor is equal to equity divided by the financial debts.

This is the “bank credit facilities” rule: The total value of all financial debts (excluding bank credit facilities) must not be greater than the equity. The financial independence ratio can be stated in various ways, all of which are consistent with this rule.

Repayment Capacity = (Financial Debts) / (Financing Capacity)

The ratio must be greater than one, to meet this rule. This rule has been introduced to give the institution financial independence, that is, equity should be more than its total debts and shareholders' contribution to the financial need of the institution should be higher than that of the lender.

Repayment Capacity Rule

This rule is based on the notion that an organization's financial obligations should not exceed three times its estimated average annual self-financing capacity. The following ratio is used by the financial decision maker as a tool to help monitor.

This ratio indicates the average time it takes a business to pay off its creditors, and it should be under 3 years. So this ratio should be less than 3. It indicates the institution's ability to pay the full amount of debts with its self-financing capacity, and thus its likelihood of becoming insolvent, hence of not being able to repay debts when they are due, which elevates the risk of insolvency. This ratio can also influence the reputation of the institution with respect to the loans, since it reflects the institution's ability to repay loans to the lenders.

To diversify the sources of financing for the institution's investment projects, the Minimal Self-Financing Rule is set as the target. It stipulates a minimum equity contribution of 1 in 3 for the projects of the institution, with the remaining 2/3 being funded by borrowing. With this kind of method, the institute can keep away from various dangers, including the rise in debt solution expenses in contrast to the income from the investment project.

Types of Financing

The types of financing for an economic institution can be divided into two main categories: Internal Financing and External Financing.

In terms of internal financing, retained earnings are the company's profits that are not distributed to shareholders but are reinvested in the company to finance new projects or expand business operations. In addition, depreciation is an allocation of funds each year to meet the cost of depreciation to the institution's fixed assets. Furthermore, an increase in capital involves the issue of fresh shares to existing shareholders or fresh share for public subscription.

External Financing: In contrast to internal financing, external financing includes several sources. First, bank financing refers to loans that are taken from banks/other financial institutions. Second, debt instruments financing includes bonds and Islamic sukuk. Furthermore, venture capital financing refers to financing that comes from investment companies or venture capital funds. In addition, crowdfunding involves raising money on a large scale online from many people. Finally, grants from government refer to funds provided by the government for a particular project.

Factors affecting the choice of financing type

Several factors can affect the choice of financing type. First, the size of the company is an important factor, as external financing is greater for large companies compared to small companies. In addition, the relationship with financing also influences the choice, as start-up companies are more likely to use internal financing and VC financing than mature companies are. Furthermore, financial needs should be considered, as the type of financing will depend on the size of the institutions financial needs. Another important factor is financing cost, as the financing cost is different for each type of financing. Finally, risk should also be considered, as this varies depending on the type of financing.

Investment Decision

An important and investment decision of financial management. Financial management usually resorts to it with the belief that it increases investment returns in order to maximize investors' wealth or maximize the market value of each share.

Definition of Investment

Investment is the allocation of money to a particular activity that is expected to yield a profit in the future. If an investment is approved in accordance with accepted standards or if the investment is likely to yield expected returns, it can be classified as an acceptable investment. Evaluation and selection for an investment is based on the cost of the funds invested in the investment project and the returns from the investment project. If that's the case, then investment can be seen as a risky bet taken by a company that can lead to profitable or unprofitable results in the future, like buying stock that might bring in yearly profits, but could also result in losses.

Characteristics of Investment

Each investment project has a number of characteristics which make it different from other projects. First, invested capital refers to the capital that is used in the project. Second, the project

duration is used to properly estimate the expected profits, and it can typically be estimated by the depreciation period of the project. Finally, the money returns received from the project refer to cash flows, which are classified as the monetary returns that are produced from the project.

Objectives of Investment

The investor tries to ensure their continued involvement and better economic relationship with the other partners. In this context, the purpose of investing is to achieve the following goals: producing a return, profit or income, and building and increasing wealth.

Types of Investment

There are two types of investments by the type of investment instrument that the investor chooses: Real Investment and Financial Investment. Real investment is investment in assets, and financial investment is investment in securities like bonds, stocks, etc., and is also called long-term investment and short-term investment. Long-term investment is investment in the form of stocks and bonds (capital investment), while short-term investment is investment in financial instruments such as treasury bills and bank deposits, and is called as cash investment.

In addition, investment can also be classified as Autonomous Investment and Induced Investment. Autonomous investment is the increase in income and national output through the private sector, public sector or foreign investment, while induced investment is the result of an increase in income.

Dividend Distribution Decision

There are other decisions that go along with investment and financing decisions which involve dividend distribution. The distribution decision set is regarded as significant for financial management because of the conflicting interest between the investors and management. While investors want a bigger share of the profits distributed to them in cash, management wants a larger share of profits retained within the company for investment growth.

Dividend Distribution Policy has an impact on the market value of the share. It is a well-known fact that the value of a share is equal to the present value of future cash flows discounted at the discount rate which is the cost of capital as represented by the following equation:

$$P_0 = \frac{D}{K-G},$$

Where: The value of the share is P D = Distributed dividends. This is the discount rate, denoted by K G is the Growth rate.

It is observed that when the numerator, i.e., the number of dividends distributed per share is increased, the value of the share of the organization can be increased. But when the dividends are distributed more, it means that the retained earnings will be less, and the organization will have less to invest in expansion and augment its productive capacity; this in turn reduces its growth rate. Hence, the best possible dividend distribution is the one which will create a balance between present dividend distribution and future expectation so as to increase the market value of the share.

The researchers find that strategic financial decisions are long term decisions about how the financial resources of universities should be allocated that yield the best long term value to meet their strategic goals. Such decisions are not just financial, they are tied to the strategic goals of the universities and are directly tied to the sustainability and competitiveness of the University. These decisions involve careful consideration of the internal and external environment, risk and return analysis, and involve investment decisions, financing decisions, dividend distribution decisions and working capital management decisions.

The student conducts previous studies and formulates a hypothesis. The student runs previous studies and develops a hypothesis.

The study by Abdel-Azim and Adel (2019) aimed to identify the nature of the disclosure of cybersecurity risks in financial reports and cybersecurity risk management programs in Egyptian companies belonging to the information technology sector, which is one of the sectors most vulnerable to cyber threats and incidents, according to the Egyptian National Cybersecurity Strategy (2011–2025). The study also aimed to compare this with the nature of disclosure of cybersecurity risk and its effect on stock prices and trading volumes of U.S. companies, including those that suffered a significant cyber attack, following the issuance of cybersecurity disclosure guidance in 2018 and the publication of a general cybersecurity risk reporting framework by the American Institute of Certified Public Accountants (AICPA) in 2017.

The study showed that the level of cybersecurity risk disclosure within the information technology firms in Egypt is low compared to that of the U.S. counterparts, as well as the level of cybersecurity risk management programs in both countries, which affects the stock prices and trading volumes negatively. In addition, the study urged the Egyptian Exchange, Financial Regulatory Authority, and the Central Bank of Egypt to immediately publish regulations and guidelines to facilitate disclosure of cybersecurity activities, cyber incidents, potential cyber threats, and cybersecurity risk management programs. It also recommended that the International Accounting Standards Board (IASB) adopt an accounting standard that would require companies to disclose their cyber security activity, cyber security risks, and cyber security risk management programs.

The study "Iraq and Cybersecurity: Opportunities and Challenges" by Al-Zubaidi and Al-Tamimi (2022) sought to determine the role of cybersecurity in the security system in Iraq, and to suggest possible solutions to enhance the concept of cybersecurity and coordinate the scientific framework of cybersecurity in the security, political, military, and economic fields. The study as a whole has led to the conclusion that information technology is one of the most critical needs for establishing secure states in an area which has never known security and stability.

This study by Youssef (2022) analysed the status of disclosure of cybersecurity risk management reports and its influence on investment and credit granting decisions in Egyptian companies listed on the Egyptian Stock Exchange (ESX), stock prices and trading volume. The study found that listed companies overall fail to adequately address the risk of cybersecurity, negatively impacting stock prices and trading volumes. In addition, the study recommended that the Egyptian Exchange, the Financial Regulatory Authority, and the Central Bank of Egypt should expedite the issuance of the required regulations and guidelines to facilitate the disclosure of cybersecurity activities, cyber incidents, potential cyber threats and cyber security risk management programs. It further called for the International Accounting Standards Board (IASB) to develop an accounting standard for disclosure of cybersecurity activities, cybersecurity risks and cybersecurity risk management programs of companies.

Alshaikh et al. (2020) studied cyber-attacks against banks and other financial institutions in Jordan and how they affect the financial statements. These cyberattacks have a direct correlation to the vulnerabilities of financial information to hackers gaining access illegally. The study sought to find the impact of cybersecurity on the quality of financial statements in selected sample of Jordanian banks because these attacks significantly affect the quality of financial statements. The findings revealed that the cyber attacks had a positive and statistically significant impact on the quality of financial statements and this impact was positively felt on the balance sheet, cash flow statement and the income statement. The findings also indicated that all of the above variables demonstrated to have a significant impact on financial statement quality other than Malicious Internal Unauthorized Access (MVIA) which did not have a statistically significant impact. Additionally, the study found that the speed and efficiency to respond to cyber incidents can reduce the impact on the institution's financial statements and its reputation.

Previous studies led to the following hypotheses

Research hypotheses reflect the research questions and research objectives presented above and are based on a review and analysis of the relevant literature.

H1: The effects of cyber security on supporting strategic financial management decisions in Iraqi Universities are statistically significant.

If there are statistically significant differences between the effects of secure digital infrastructure on improving the speed and accuracy of financial management decisions, H2 is accepted. If the effect of secure digital infrastructure on improving the speed and accuracy of financial management decisions is statistically significant, H2 is accepted.

H3: The use of cybersecurity in financial systems and the relationship between financial systems and cybersecurity positively impacts the enhancement of risk response, along with the achievement of strategic goals in financial systems, and is statistically significant.

H4: The use of cybersecurity practices significantly affects the quality of strategic financial management decision making within Iraqi universities.

2. Method

The researchers adopt the descriptive-analytical approach in a field study, with a questionnaire as the main tool for collecting data to describe and analyze the impact of cyber security on supporting decisions in strategic financial management. The phenomenon being studied was described, analyzed and data collection on the study sample was conducted through the use of a questionnaire and the data were analyzed statistically to arrive at the results of the proposed hypotheses. The researchers also used the "inductive approach" to study how cybersecurity influences the strategic financial management decisions by analyzing several previous research articles, periodical publications, scientific journals, and scholarly articles on cyber risks and how they can be mitigated. In this section, the design of the Exploratory Study is described as follows.

2.1. Population and Sample of the Study

The population of the study includes most of the Iraqi universities. The information for the study was retrieved from the respondents after identifying and defining the target population (n=200). A random sample of 186 respondents was selected, which is 93% of the population size. The sampling and analysis unit for this study encompasses faculty, information systems staff, administrative and financial staff. The descriptive data in Table (1) reflect the descriptive data of the study sample based on the variables (gender, age, educational level, job title and duration of service).

Table 1. Characteristics of the Research Sample Participants

Variable	Categories	Frequency	Percentage (%)
Sex	Mal	120	%64.5
	Female	66	%35.5
Age	Less than 30 years	66	%35.5
	30 -39 years	49	%26.3
	40 – 49 years	48	%25.8
	More than 50 years	23	%12.4
Attainment	Bachelor	50	%26.9
Educational	Master	72	%38.7
	Doctorate	36	%19.4
	Other	28	%64.5
Job Title	Faculty Members	91	%35.5
	Information Systems Officer	42	%35.5
	Administrative and Financial Staff	53	%26.3
Years of Service	Less than 5 years	65	%34.9
	From 5 to 10 years	49	%26.3
	More than 10 years	72	%38.7
Total		186	100%

Source: Prepared by the Researchers.

As can be seen from the previous table, males make up the largest amount of the sample as the percentage of the sample is (64.5%). In terms of age, under 30 years old had the highest percentage (35.5%). When it comes to education, the highest number of respondents had a Master's degree (38.7%). As far as job title is concerned, faculty members had the highest number (48.9%) and as far as years of service is concerned, the highest number (38.7%) was in the category of more than 10 years of service.

The researchers realized that the subjects of the study are mainly males, and the younger age group has great interest in the role of cybersecurity in supporting strategic solutions for financial

management in Iraqi universities. In addition, many of the respondents hold an advanced academic qualification and this is a much sought after qualification in the academic realm. This makes their views more believable and an expression of their knowledge and experience in the subject matter of the study.

2.2. Data Collection Instrument and Methods

A questionnaire was developed to address the research hypotheses and used to rate the answers of the sample of the study according to the proposed questions using a set of evaluative statements to attain the objectives of the study. The researchers applied the questionnaire development methodological techniques, which are the most meaningful ones:

The items on the questionnaire were grouped into four classes, each class being a major dimension of the study variables.

The researchers used the 5 point Likert scale to design the questionnaire. Responses for each item were categorized into five responses and a weighted score assigned, with a score of 5 given if the respondent agreed strongly, 4 if they agreed, 3 if there was no opinion, 2 if they disagreed, and 1 if they disagreed strongly.

Furthermore, various statistical methods were used to analyze data and to test the hypotheses. These comprised Cronbach's Alpha to evaluate the internal consistency and reliability of the measuring scales utilized in the study, descriptive statistical methods including the mean, median and standard deviation were also used, while Pearson correlation analysis was used to measure the strength of the relationship between the variables of the study.

3. Results and Discussion

3.1. Descriptive Statistical Analysis

Reliability test is a means of assessing the degree of trustworthiness of the findings from the questionnaire. For this reason, Cronbach's Alpha coefficient and the validity coefficient were used, because they are generally accepted as the most widely used measures for the internal consistency of the study variables. Generally, it is accepted that the value of Cronbach's alpha for questionnaires should not be lower than 0.6, and the higher the value, the more reliable and consistent the questionnaire's results are. This test was performed and the results are given below.

Table 2. Results of Cronbach's Alpha and Validity Coefficient Tests for the Research Variables

Code Variables	Study variables	Number of Items	Cronbach's Alpha Coefficient	Coefficient Validity
x_1 - x_{10}	The Impact of Cybersecurity on Supporting Strategic Financial Management Decisions in Iraqi Universities.	10	0.808	0.898
$x_{11} - x_{20}$	The Impact of Secure Digital Infrastructure on Improving the Speed and Accuracy of Financial Management Decisions	10	0.640	0.8
$x_{21} - x_{30}$	The Integration of Cybersecurity and Financial Systems in Enhancing Risk Response and Achieving Strategic Objectives	10	0.677	0.823
$x_{31} - x_{40}$	The Application of Cybersecurity Practices to the Quality of Strategic Financial Management Decision-Making in Iraqi Universities	10	0.712	0.844
Cronbach's Alpha Value		40	0.767	0.876

Source: Analysis Results of SPSS

The reliability coefficient in the previous table was (767,0) for all variables and also the validity coefficient was (876,0) for all the variables. This is a high-level statistical measure that will give good consistency between the study variables, good confidence on the variables and confirmation that they are an appropriate set for the rest of the analysis.

3.2. The Impact of Cybersecurity on Supporting Strategic Financial Management

Decisions in Iraqi Universities: The researchers analyzed and examined the answers of the individuals who were asked to determine the impact of cyber security on facilitating decisions in strategic financial management in Iraqi universities, based on the following table (descriptive statistics):

Table 3. Statistical Analysis Results on the Impact of Cybersecurity on Supporting Strategic Financial Management Decisions in Iraqi Universities

Serial	Statements	Arithmetic Mean	Median	Standard Deviation
X_1	Cybersecurity affects the accuracy of administrative financial decision-making in Iraqi universities	3.87	4	0.989
X_2	Cybersecurity helps reduce financial errors	3.85	4	1.068
X_3	Data protection enhances confidence in the information used in decision-making	3.85	4	1.105
X_4	Cybersecurity reduces financial risks	3.95	4	1.099
X_5	A secure digital environment helps in making fast financial decisions	3.74	4	1.152
X_6	Cybersecurity increases the effectiveness of financial analysis	3.80	4	1.104
X_7	Cybersecurity supports the implementation of financial contingency plans	3.72	4	1.114
X_8	Cybersecurity affects strategic spending priorities	3.68	4	1.136
X_9	Cybersecurity enables greater flexibility in resource allocation	3.64	4	1.174
X_{10}	Cybersecurity contributes to achieving long-term financial management objectives	3.63	4	1.146
Total		3.773	4	1.109

Source: Results of SPSS analysis

From the above table, the effect of cybersecurity on supporting the strategic financial management decision in Iraqi universities is clear, with the overall mean being (3.773), the total median (4), and the standard deviation (1.109) showing the importance of cybersecurity's impact on financial management decisions.

3.3. How digital infrastructure helps to optimize the decision-making process in financial management

The researchers analyzed the opinions of the respondents based on descriptive statistics as shown in the following table to determine the impact of cybersecurity on supporting strategic financial management decisions in Iraqi universities.

Table 4. Statistical analysis results regarding the impact of secure digital infrastructure on improving the speed and accuracy of financial management decisions.

Serial	Statements	Arithmetic Mean	Median	Standard Deviation
x_{11}	Strong protection systems are available for strategic financial data	4.22	4	0.894
x_{12}	Security systems are updated regularly	3.73	4	1.067
x_{13}	Encryption techniques are used for sensitive Data	3.91	4	1.161
x_{14}	Data backups are created and stored periodically	3.62	4	1.221
x_{15}	The organization relies on effective firewalls	3.82	4	1.156
x_{16}	The organization relies on real-time system monitoring to detect any intrusion	3.68	4	1.218
x_{17}	Vulnerabilities are tested Periodically	3.94	4	0.886
x_{18}	There are clear policies for accessing financial information	3.96	4	0.917
x_{19}	There is an internal unit responsible for cybersecurity management	4	4	0.864
x_{20}	A separate budget is allocated to develop the security infrastructure	3.95	4	1.007
Total		3.883	4	1.03

Source: Results of SPSS analysis

From the above table, it is clear that SDI has a high impact on the speed and accuracy of financial management decisions with a mean of (3.883), a total median of (4), and a standard deviation of (1.03) which shows that SDI plays a significant role in enhancing the speed and accuracy of financial management decisions.

3.4. Cyber Security integration to Financial Systems to improve risk response and strategic goals

The researchers used the descriptive statistics mentioned in the following table to analyze the respondents' views regarding the impact of cybersecurity on supporting strategic financial management decisions in Iraqi universities.

Table 5. Statistical analysis results regarding the integration between cybersecurity and financial systems in enhancing risk response and achieving strategic objectives

Serial	Statements	Arithmetic Mean	Median	Standard Deviation
x_{21}	Cybersecurity systems are integrated with the strategic financial administrative system	3.93	4	0.930
x_{22}	Information is exchanged efficiently between administrative and financial Departments	3.80	4	0.980
x_{23}	Integration supports response to cybersecurity attacks	3.86	4	0.954
x_{24}	Integration contributes to reducing gaps between data and financial outputs	3.83	4	1.002
x_{25}	Integration provides a comprehensive view of business risks	3.91	4	0.932
x_{26}	This integration contributes to enhancing the quality of financial performance	3.82	4	0.964
x_{27}	Plans are coordinated between the cybersecurity management and the financial management	3.92	4	0.978
x_{28}	Integration leads to the development of more secure digital financial solutions	3.97	4	0.847
x_{29}	Integration contributes to reducing potential financial losses	3.84	4	0.979
x_{30}	Integration enhances the organization's preparedness to address administrative, financial, and security crises	3.87	4	0.921
Total		3.87 5	4	0.948

Source: Results of the SPSS data analysis

An overall mean of (3.875), median of (4) and standard deviation of (o.948) is observed in the previous table for the level of integration of cybersecurity and financial systems in the enhancement of risk response and achievement of strategic goals. This embodies the significance of integrating cybersecurity and administrative and financial systems to enhance risk response and strategic goals and then to serve academic and educational interests.

3.5. How far is the application of cyber security practices from the quality of strategic financial management decision making in Iraqi universities?

To get a better idea of how the respondents view cybersecurity and its effects on supporting strategic financial management decisions in Iraqi universities, the descriptive statistics in the following table were analyzed:

As shown in the table 6, the percentage of applying the cyber security practices with regard to the quality of strategic financial decisions in Iraqi universities is high, with a mean of (3.882) and a standard deviation of (0.963). This underlines the necessity of the use of cyber security to enhance the quality of strategic financial decision making in Iraqi Universities which makes it more accurate and protected from data breaches, and more secure.

Pearson correlation analysis: This presents and analyzes the results obtained from simple correlation coefficient between the study dimensions to find the strength of the relationship, the direction of the relationship and the significance of the relationship among the study variables. The higher the correlation coefficient the greater the relationship between these variables is. If it is positive (+), it is a direct relationship; if it is negative (-), it is a diverse or inversely proportional relationship. Table 2 shows the correlation matrices of the major dimensions of research variables.

Table 6. Statistical analysis results regarding the application of cybersecurity practices on the quality of strategic financial decision-making in Iraqi universities

Serial	Statements	Arithmetic Mean	Median	Standard Deviation
X_{31}	Strategic financial management is based on forecasting and planning, investment and financing decision- making, as well as coordination and monitoring, and risk management	3.90	4	0.967
X_{32}	Cybersecurity contributes to coordinating services, facilitating access to them, and identifying how to benefit from them, thereby achieving strategic financial objectives	3.95	4	0.993
X_{33}	Among the determinants of successful strategic performance are fewer and faster processes, along with ensuring information security and privacy	3.92	4	0.952
X_{34}	Strategic financial management objectives are achieved through profit maximization, maximizing organizational value, and maximizing social and financial returns	3.89	4	0.941
X_{35}	Organizations adopt an information technology strategy to enhance their competitiveness in the market	3.74	4	0.901
X_{36}	The financial function is considered an important function; therefore, financial management is placed at the highest levels of organizational structure due to its importance	3.90	4	0.978
X_{37}	Strategic financial management permeates all areas of activities	3.68	4	1.004
X_{38}	Strategic financial decisions are often binding, which requires great caution when making them	3.87	4	1.034
X_{39}	Some strategic financial decisions determine the success or failure of the organization	3.94	4	0.951
X_{40}	Financial management is an integral part of organizational management	4.03	4	0.915
Total		3.882	4	0.963

Source: Results of SPSS data analysis

Table 7. Correlation matrix of the study variables

Research Dimensions	The Impact of Cybersecurity on Supporting Strategic Financial Management Decisions in Iraqi Universities	The Impact of Secure Digital Infrastructure on Improving the Speed and Accuracy of Financial Management Decisions	The Integration of Cybersecurity and Financial Systems in Enhancing Risk Response and Achieving Strategic Objectives	The Application of Cybersecurity Practices to the Quality of Strategic Financial Management Decision-Making in Iraqi Universities
The Impact of Cybersecurity on Supporting Strategic Financial Management Decisions in Iraqi Universities	1	0.645	o.419	0.379
The Impact of Secure Digital Infrastructure on Improving the Speed and Accuracy of Financial Management Decisions		1	0.542	0.470
The Integration of Cybersecurity and Financial Systems in Enhancing Risk Response and Achieving Strategic Objectives			1	0.731
The Application of Cybersecurity Practices to the Quality of Strategic Financial Management Decision-Making in Iraqi Universities				1

Source: SPSS Analysis Results

From the table 7, it is clear that all the essential dimensions of the variables of the study are showing positive and statistically significant correlation among themselves with significant level of (0.05). The results also show that when the significance value is > (0.05) the data are not normally distributed; when the significance value is < (0.05) the data are normally distributed.

The correlation coefficients between the dimension of the impact of Cyber security on supporting strategic financial management decisions in Iraqi universities with the other dimensions were (0.645, 0.419 and 0.379), respectively. Likewise, the correlation coefficients between the dimension secure digital infrastructure with the other dimensions in improving the speed of taking financial management decisions and the accuracy of financial management decisions were obtained (0.542, 0.470). Further, the correlation coefficient between the dimension of integrating cybersecurity and financial systems in improving risk response and strategic goals, and other dimensions was nearly (0.731).

The other way around, these relationships validate the validity of the items in the questionnaire in measuring the main dimensions of the research topic since they show a real relationship which could not have occurred by chance.

4. Conclusion

The study aimed to test the impact of cybersecurity on supporting strategic financial management decisions in Iraqi universities. The main research results are presented from both theoretical and exploratory (empirical) aspects. Cybersecurity refers to a collection of policies, procedures, and technologies designed to protect information systems and digital data from internal and external threats. It does not only cover technical aspects but also includes building awareness among people, risk management, and organizational structure development, with the goal of protecting digital assets from sophisticated types of attacks and maintaining business continuity and integrity in an evolving digital landscape. The exploratory study results showed that the reliability for all variables was high (0.767), while all variables had a validity coefficient of 0.876, which is considered statistically good. This indicates the extent of similarity between the variables studied, raises confidence in the variables, and increases their validity. The statistically significant positive effect means that there is a strong and meaningful correlation among the main dimensions of the study variables, and all relationships are statistically significant at the 0.05 level of significance. When the significance value is > 0.05, the data are not normally distributed; otherwise, the data are approximately normally distributed. The correlation coefficients between the dimension of cybersecurity supporting strategic financial management decisions in Iraqi universities and the other dimensions were 0.845, 0.419, and 0.379, respectively. The correlation coefficients between the dimension of secure digital infrastructure (SDI) and other dimensions in improving financial management decisions that can be made quickly and accurately were 0.542 and 0.470. Furthermore, the correlation coefficient of cybersecurity integration with financial systems' role in risk response and strategic goal achievement was 0.731 with the other dimensions. These relationships validate the value of the questionnaire items in measuring the main dimensions of the research topic, as they show true relationships that are not due to chance. Therefore, it is important to have cybersecurity systems to support strategic financial management decisions in universities, enabling stakeholders to make appropriate decisions, defend against cyberattacks and security threats, and identify solutions and the consequences of those decisions. Universities also need to increase awareness of the significance of cybersecurity and the risks it poses to university operations and results. In addition, universities need to establish proper security policies and controls to enable cybersecurity measures that protect all data and information related to the curriculum, students, and staff, thereby supporting strategic financial management decisions in the event of cyber risks.

References

Ab Abbas, H. A., & Shaker, A. M. (2022). Cybersecurity challenges and policy gaps in Iraqi higher education institutions. *Journal of Information Security, 13*(2), 45–59.

Abdel-Azim, T., & Adel, D. (2019). The impact of cybersecurity risk disclosures in financial reports on stock prices and trading volumes: A comparative study. *Journal of Accounting and Auditing*, (2), 439–487.

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, *25*(2), 357-370.

Al Shamsi, A. A. (2019). Effectiveness of cyber security awareness program for young children: A case study in UAE. *International Journal of Information Technology and Language Studies, 3*(2), 8–29.

Al-Ajlan, G. M. (2024). Cybersecurity and its role in supporting financial management decisions: An applied study on Arab universities. *Arab Journal of E-Management, 14*(1), 115–134.

Al-Baghdadi, M. (2021). Economics of cybersecurity in the banking sector. *Journal of Legal and Economic Research, Mansoura University*, *76*, 1446-1513..

Alsakini, S. A. K., Alawawdeh, H. A., & Alsayyed, S. (2024). The impact of cybersecurity on the quality of financial statements. *Applied Mathematics & Information Sciences, 18*(1), 169–181. http://dx.doi.org/10.18576/amis/180117

Alshaikh, M., Maynard, S. B., & Ahmad, A. (2020). Towards a model for strategic information security governance. *Journal of Information Security and Applications, 50*, Article 102419. https://doi.org/10.1016/j.jisa.2019.102419

Al-Zubaidi, Z. K. A., & Al-Tamimi, M. A. M. (2022). Iraq and cybersecurity: Opportunities and challenges. *Wasit Journal for Human Sciences, 18*(51).

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies, 23*(3), 1177–1206. https://doi.org/10.1007/s11142-018-9452-4

Badawy, H. A. E. S. (2021). The impact of assurance quality and level on cybersecurity risk management program on non-professional Egyptian investors' decisions: an experimental study. *Alexandria Journal of Accounting Research*, *5*(3).

Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial auditing journal*, *33*(4), 360-376. https://doi.org/10.1108/MAJ-02-2018-1804

Cram, W. A., D'arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy Compliance1. *MIS quarterly*, *43*(2), 525-553.

Farag, H. K., Imam, D. H., Muhammad, M. F., & Muhammad, H. (2017). *E-auditing: Impacts, challenges, and applications*. University Education House for Printing and Publishing.

Florakis, C., Louca, C., Michaely, R., & Weber, M. (2020). Cybersecurity risk. *SSRN*. http://ssrn.com. https://doi.org/10.2139/ssrn.3767307

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity accounting research. *Managerial Auditing Journal, 34*(7), 808–834. https://doi.org/10.1108/MAJ-09-2018-2004

Hartmann, C. C., & Carmenate, J. (2021). Academic research on the role of corporate governance and IT expertise in addressing cybersecurity breaches: Implications for practice, policy, and research. *Journal of Information Systems, 35*(2), A9–A23. https://doi.org/10.2308/CIIA-2020-034

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2018). *What is the impact of successful cyberattacks on target firms?* (No. w24409). National Bureau of Economic Research. https://doi.org/10.3386/w24409

Kelton, A. S. (2019). Cybersecurity and corporate risk management: Insights and implications. *Journal of Information Systems, 33*(3), 85–104.

Khalid, A., Saleem, B. A., Al-Emran, M., & Zainal, A. (2022). Human factors influencing cybersecurity behavior: A systematic review. *Computers & Security, 112*, Article 102527. https://doi.org/10.1016/j.cose.2022.102527

Li, H., No, W. G., & Wang, T. (2019). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems, 30*, 40–55. https://doi.org/10.1016/j.accinf.2018.06.003

Oqaili, I. (2014). *Financial management*. Tlemcen University.

Perols, R. R., & Murthy, U. S. (2021). The impact of cybersecurity risk management examinations and cybersecurity incidents on investor perceptions and decisions. *Auditing: A Journal of Practice & Theory*, *40*(1), 73-89. https://doi.org/10.2139/ssrn.3112872

Richardson, V., Watson, M. W., & Smith, R. E. (2019). Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Systems, 33*(3), 227–265. https://doi.org/10.2308/isys-52379

Schiliro, F. (2022). *Towards a contemporary definition of cybersecurity*. Australian Defence Force Academy, University of New South Wales & Macquarie University.

Shahimi, S. (2018). Building a research model and hypotheses development for internal audit consulting: insights from literature and findings of exploratory interviews. *International Journal of Management Excellence*. https://doi.org/10.17722/ijme.v10i2.959

Sharma, P. P., Mishra, N., & Avinash, A. (2023) Revisiting Cyber Security Literature Post-Pandemic Rapid Digitalization Using the Tccm Literature Review Method.

Siti, R. (2023). Cybersecurity strategies for higher education institutions: A systematic review. *Technology in Society, 73*, Article 102258. https://doi.org/10.1016/j.techsoc.2023.102258

World Economic Forum. (2017). *The global risks report 2017* (12th ed.). http://www3.weforum.org/docs/GRR17_Report_web.pdf

Yassin, S., Al-Hajj, Z. D., & Fares, B. (2024). Financial management in the enterprise: A field case study at the Algerian Pipe Industry Company (ALFABIPE) Ghardaïa [Unpublished master's thesis]. Ghardaïa University.

Youssef, A. A. K. (2022). The impact of cybersecurity on the sustainability of educational institutions: A field study at Iraqi universities. *Journal of Financial and Administrative Sciences, 19*(2), 56–81.

Zahwani, R., Kheir El-Din, S. F., & Bouafia, M. (2017). The role of financial management in financial decision-making. *Journal of Administrative and Financial Sciences, 1*(1).