Next Scientists
Journal of Management and Economics

TYPE Original Research
PAGE NO. 6-23
DOI 10.55640/jme-05-08-02

The Appointment Of Cybersecurity In Combating The Phenomenon Of Accounting Fraud

Lect. Dr. Basim Mohammed Hussein

General Directorate of Education, Al-Najaf Al-Ashraf, Iraq

Lect. Ibrahim Hilal Abdul-Sadah Mubarak

General Directorate of Education, Al-Najaf Al-Ashraf, Iraq

Lect. Dr. Taisir Jawad Kazem Sultan

General Directorate of Education, Al-Najaf Al-Ashraf, Iraq

OPEN ACCESS

SUBMITED 30 June 2025
ACCEPTED 29 July 2025
PUBLISHED 31 August 2025
VOLUME Vol.05 Issue08 2025

Abstract: The use of cybersecurity to combat accounting fraud is a positive indicator of companies operating in the Iraqi environment adopting such secure policies, which most major companies adopt to protect digital data and information from unwanted phenomena. The researchers used a set of technologies underlying cybersecurity, including encryption technology, access control, and intrusion monitoring systems, to combat any negative phenomena. For this purpose, the researchers designed a robust scientific questionnaire with two axes. The results, in which 77 respondents participated, showed that there is a direct relationship between activating and adapting cybersecurity as an essential policy to protect corporate assets from attacks and threats that companies may be exposed to, including the phenomenon of accounting fraud. One of the most important recommendations was the need for companies operating in the Iraqi environment to adopt contemporary methods and policies in the field of accounting information systems to protect their electronic assets. Cybersecurity is one of the most important of these policies that reduces the commission of negative phenomena to which these companies are exposed.

Keywords: Words: Information Security, Cybersecurity, Encryption, Accounting Fraud, and Pressures.

Introduction: Information security is a contemporary digital topic that requires significant attention from companies seeking success and continuity in a challenging business environment. Cybersecurity plays a prominent role as a comprehensive policy for protecting companies' electronic environments, including their essential data and information. This policy provides a protective cover and shield against attacks, threats, risks, and negative phenomena that must be addressed resolutely to provide a safe environment against these undesirable effects, including the phenomenon of accounting fraud.

Chapter One: Scientific Research Methodology

1-1 Research Problem: Companies attempt to protect their assets from manipulation and fraud, as well as protect information, which represents the fundamental foundation for the success and sustainability of companies. Without this information, companies become weak, and various fraudulent phenomena are prevalent, some of which are committed by company management and others by employees. These phenomena are a result of motives that encourage accounting fraud, including financial pressures, opportunities due to weak internal control systems, and justifications offered by some employees based on comparison with their peers. Accordingly, the research problem can be formulated with the following question: Does the use of a cybersecurity policy contribute to combating the phenomenon of accounting fraud?

1-2 Significance of the Research: The importance of the research lies in addressing the topics of digital accounting information systems, auditing, and oversight that mimic the reality of the contemporary business environment. Cybersecurity, as a modern policy, directs the attention of those in charge of managing Iraqi companies toward providing secure methods, means, and measures to protect accounting data and information from fraudulent phenomena, including accounting fraud, which occurs as a result of the presence of pressures, opportunities, and justifications. These elements are mitigated by providing cybersecurity oversight tools to enhance security and combat the phenomenon of accounting fraud.

1-3 Research Objectives: The research aims to achieve a set of objectives, the most important of which are the following:

1. Identify the literature on cybersecurity policy.

2. Identify the literature on the phenomenon of accounting fraud.

3. Establish the conceptual foundation for employing cybersecurity as an essential policy in combating the phenomenon of accounting fraud.

4. Designing a validated scientific questionnaire with principal axes and formulating essential questions to obtain the opinions of the audience of respondents from professors and professionals in public and private universities and prestigious government institutions to extract the results of the applied aspect of the research.

1-4 Research Hypothesis: The research is based on the null hypothesis, which states the following:

There is no statistically significant effect of the use of cybersecurity in combating the phenomenon of accounting fraud.

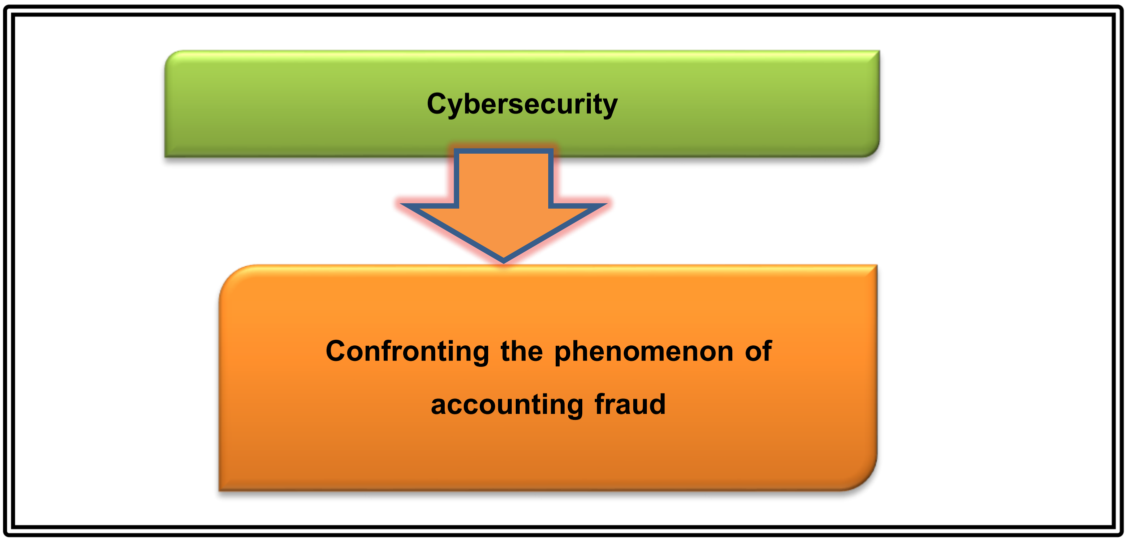
1-5 Research Limits: The research limits can be divided into spatial and temporal limits, as follows:

1-5-1 Spatial Research Limits: The spatial limits of the research are represented by a sample of Iraqi public and private universities and government institutions to which the respondents, academics, and professionals belong.

1-5-2 Temporal Research Limits: The temporal limits of the research are represented by the fiscal year in which the questionnaire was formulated, which is 2025.

1-6 Research Model: A research model can be formulated that combines the research variables, as follows:

Figure (1): Procedural Research Model



المصدر : من إعداد الباحثين .

Chapter Two: The Theoretical Framework of the Research

Requirement One: A Philosophical Introduction to Cybersecurity

1-1 The Concept of Security:

1. Security can be defined in two synonymous ways. From a technical perspective, it can be defined as all the means, tools, and procedures necessary to ensure the protection of information from internal and external threats. From a legal perspective, it can be defined as the study of the methods and measures necessary to protect the confidentiality and availability of information and combat activities that attempt to harm it or exploit its systems to commit fraud (Razzaq, 2024: 24-25). 1-2 Basic principles governing information security:

2. The official bodies responsible for issuing local and international standards seek to establish that information systems and their security are based on the availability of the following trinity (Steinbart and Marshall, 2018: 344-346):

3. Reliability: Ensuring that information security is not disclosed or accessed except by authorized persons, whether stored on a physical medium or transmitted via communications.

4. Availability: Ensuring the continuity of the operation of information systems with all their components and the continued ability to interact with them, ensuring the provision of services and information to users upon request without delay and without being subject to denial of use or access.

5. Integrity and content integrity: Ensuring that information content is complete and correct and has not been modified, destroyed, or tampered with at any stage of processing or exchange, whether illegally, intentionally, or accidentally.

It is worth noting that these principles are based on three fundamental concepts:

1. Security is an administrative issue, not a technical one.

2. The ideal security model is time-based

3. The concept of defense in depth is one of the most critical security principles.

1-3Information security components:

Information security represents a systematic, organized approach based on four interacting components that cannot be dealt with individually and independently. These components are (Awadallah, 2018: 54-55):

1. Processes: Processes are the primary and indispensable component of any security system. They are essential and continuous in nature. Processes are implemented in an organized manner and are regularly reviewed within the framework of cumulative experience to eliminate errors and address potential risks.

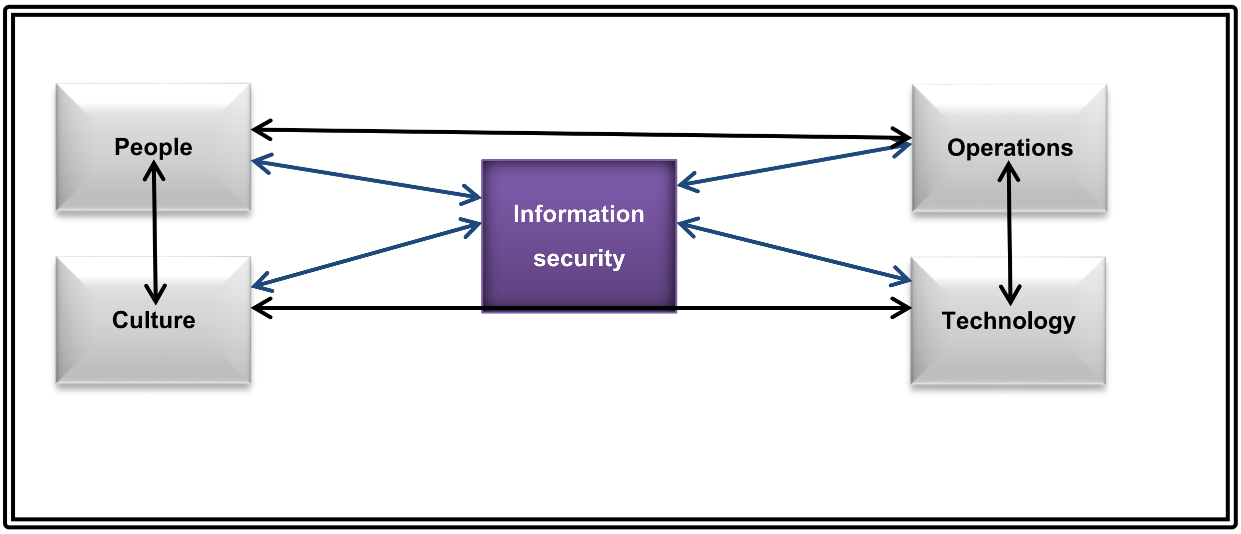
2. Individuals: Individuals perform operations and services, and their presence is required in appropriate numbers, with proper specializations, skills, experience, and realism.

3. Technology: The technology market is characterized by a large number of producers, suppliers, sellers, and distributors. These companies may merge into significant partnerships or may lose out and exit the business market.

4. Culture: The cultural component is linked to the interpretation of the business environment and relates to the company's ethics toward the community in which it operates. Company management plays a crucial role in preserving and promoting a company culture that aligns with the community's culture with which it interacts.

Figure (2): Components of Information Security

Figure (2): The Four Components of Information Security



.

Source: Prepared by researchers.

The figure above illustrates how the components of information security are interconnected. Disconnecting one element from another can lead to dysfunction.

1-4 The concept of cybersecurity:

Cybersecurity is often used interchangeably with information security. However, cybersecurity is not necessarily limited to protecting cyberspace itself; it also includes protecting those operating within it and any assets accessible through it. Cybersecurity encompasses technologies, processes, and controls designed to protect systems, networks, and data from cyberattacks. Effective cybersecurity reduces the risk of cyberattacks and protects communities, organizations, and individuals from unauthorized access to, or exploitation of, systems, networks, and technologies. Cybersecurity is a comprehensive concept that encompasses information security and assurance. As a result, cybersecurity includes the protection of information that is evaluated and transmitted over any computer network (Haapamäki & Sihvonen, 2019, p. 812). More importantly, the US Department of Defense (the Pentagon) has provided a precise definition of the term (cybersecurity), describing it as (all organizational measures necessary to ensure the protection of information in all its electronic and physical forms, from various crimes, attacks, sabotage, espionage, and accidents). While the European Declaration on Cybersecurity defines it as "the ability of an information system to resist hacking attempts or unexpected incidents targeting data," according to the definition issued by the International Telecommunication Union (ITU) report on "Trends in Telecommunications Reform," cybersecurity is defined as "a set of technical, organizational, and administrative means used to prevent unauthorized use, misuse, and recovery of electronic information and the communications and information systems containing them, to ensure the availability and continuity of information systems, enhance the protection, confidentiality, and privacy of personal data, and take all necessary measures to protect citizens and consumers from risks in cyberspace." It is worth noting that the definition of cybersecurity is relative and depends on the nature of each country and entity's perception and understanding, each according to its vision, strategy, and ability to exploit available advantages and confront potential risks in this field. Based on its objectives, cybersecurity can be defined as the activity that ensures the protection of human and financial resources associated with communications and information technologies, and ensures the possibility of limiting losses and damages resulting from them if risks and threats materialize. It also allows for the situation to return to normal as quickly as possible, provided that the wheel of production does not stop, and that the damage does not turn into permanent losses. Cybersecurity also represents the comprehensive activity of the state, its operations, capabilities, or its information and communications systems, such that the information contained therein is protected from any motive for harm or use (Khadidja, Sebkhaoui, 2024: 614-615).

Other definitions of cybersecurity include the practice of protecting systems, networks, and programs from digital attacks that typically aim to access, alter, or destroy sensitive information, extort money from users, or disrupt business operations (Al-Fadl et al., 2024: 20). It can also be defined as the activity that secures the protection of human and financial resources associated with information and communications technologies, ensures the possibility of limiting losses and damages in the event of risks and threats being realized, and enables the situation to return to its previous state as quickly as possible, so that the wheel of production does not stop and the damages do not turn into permanent and ongoing losses (Abu Al-Khair, 2023: 11). From another perspective, cybersecurity can be defined as the protection of assets from the risks posed by the use of information and communications technology, which forms the basis of cyberspace. The NIST framework provides an essential definition of cybersecurity: the process of protecting information by preventing, detecting, and responding to cyber threats and attacks (Mahrous and Saleh, 2022: 445). 1- 5 Cybersecurity Components:

Comprehensive cybersecurity frameworks consist of several interconnected components that work together to provide adequate protection against cyber threats. The main components (Fatoki, 2023: 506) include the following:

1. Secure locks and alarms: Various technologies are used to maintain network security, just as a home security system keeps the security of your home. It ensures that only the appropriate people have access to the network, prevents unauthorized access, and prevents anyone from stealing or spying on transmitted information.

2. Secure data protection: Protecting data means taking steps to ensure that no one can view, use, or take it without permission. This includes placing it in a locked box, storing it in a secure location, and ensuring that it is permanently backed up in case it is lost or broken.

3. Strict control system: Only specific people are allowed access. The system uses passwords, fingerprints, and additional security measures to ensure that only the appropriate people can access the system and use its contents. The system also ensures that people only have access to what they need and cannot do anything they are not authorized to do.

4. Effective Response to Threats and Risks: When a threat occurs, such as a cyberattack, we have a plan to detect and stop it quickly. We use specialized tools to investigate and fix the problem and ensure it does not recur. Acting swiftly and efficiently is critical to maintaining computer integrity and preventing further incidents or threats.

1-6 Cybersecurity Objectives:

There are several objectives that a company's cybersecurity can achieve, perhaps the most prominent of which (Babaker, 2025: 133-134) are the following:

1. The primary objectives of information protection are to ensure the confidentiality, integrity, and availability of information. Any event or problem that threatens the security triangle (confidentiality, integrity, and availability of information) represents a security threat that must be addressed and resolved, or mechanisms or procedures must be put in place to avoid or mitigate its effects.

2. Security must be integrated into software and operating systems to ensure the required level of protection, as companies now face increasing risks, such as cyberattacks

1. Information security has become essential because it affects companies in almost all fields and industries. Data breaches affect millions of customers and cost companies millions of dollars.

2. We don't need to discuss the importance of information security because it has become a given in this digital age. Information security is of paramount strategic importance, and senior management plays a pivotal role in establishing and managing information security within a company.

1-7 Cybersecurity Oversight & Contemporary Technologies:

Successive levels of oversight, provided by preventive, diagnostic, and corrective oversight, can be used to contribute to delivering cybersecurity oversight of control systems and ensuring their reliability. The table below shows the type of oversight and examples of oversights that fit these three types, as follows:

Table (1): Levels of Cybersecurity Oversight.

Common control examples	Type of control
Authentication control. Authorization control. Training. Physical contact control. Remote contact control.	Preventive

Firewall procedures.	
Recorded observations. Intrusion monitoring systems. Management reports. Cybersecurity testing process.	Diagnostic
Computer Emergency Response Teams. Cybersecurity Officer. Package Management.	Corrective

Source : Romney , Marshall B. , Steinbart , Paul John , Scott , L . Summers & David , A. Wood , Accounting Information Systems – Global Edition , Fifteenth Edition , Pearson Education , 2021 , page (366)

Some contemporary secure techniques that can be used to enhance cybersecurity are (Steinbart and Marshall, 2018: 351-377):

First, encryption: The process of changing natural text from readable text to an unreadable technical language called ciphertext, and then inverting this process, converting the ciphertext back to plaintext. The key and algorithm work together to convert the plaintext to ciphertext and decrypt the ciphertext, returning it to plaintext. Computers display the plaintext and ciphertext as a string of binary codes in the format (0X & 1S). The key is also a type of fixed-length double code. For example, a 128-bit key consists of a 128-bit string or a small one of the type 0X & 1S. The strength of encryption depends on three important factors:

1. The length of the encryption key.

2. The main management policies.

3. The nature of the encryption algorithm. Second: Access Control (Authentication): Authentication controls the authorization and authentication of users and machines. Every workstation, printer, or calculator requires a network interface card (NIC) to connect to the company's internal network. Each NIC has a unique identifier, known as a MAC address.

Third: Intrusion Detection Systems (IDS): Intrusion detection systems (IDSs), also known as intrusion detection systems (IDSs), record performance logs of network traffic that is allowed to pass through the firewall. They then analyze the performance logs to identify relationships between successful intrusion attempts. The most common analysis method used by IDSs is to compare their performance logs with a database containing traffic samples associated with known attacks, just as antivirus software (A-V) systems compare code snippets with a database of known viruses. An alternative approach used by more advanced IDSs is to first build a model representing normal network traffic and then use various statistical methods to identify unusual or anomalous behavior. The Second Requirement: A Philosophical Introduction to the Phenomenon of Accounting Fraud

1-1 The Concept of Accounting Fraud:

Fraud is one of the most prominent challenges facing companies through the use of illegal methods and manipulation of financial data, as well as the use of forgery, embezzlement, and manipulation to achieve illegitimate desires. This impacts the credibility of corporate reports and, in turn, leads to significant financial losses.

Fraud has been defined as the intentional presentation of misleading information about material facts with the aim of convincing someone to believe and act upon a falsehood, resulting in loss or damage. Fraud is committed by exaggerating revenues and assets, understating expenses and liabilities, and providing false disclosures (Louwers et al., 2021: 126). Fraud is the deception of someone to obtain an unfair or illegal benefit. According to the Association of Certified Fraud Examiners (ACFE), . The International Reference in Fraud Detection (Amat, 2019:1) identifies the main types of accounting fraud as follows:

1. Theft of assets: cash, expensive goods, inflated expenses, and employees receiving salaries without working.

2. Corruption: conflicts of interest, bribery, illicit gifts, and extortion.

3. Accounting manipulation: overstating assets, liabilities, expenses, and income (ACFE 2016).

2-2 Adjustment of Financial Information for Companies:

Accounts can be adjusted to reflect accounting observations or actual transactions, which can be legal or illegal (Amat, 2019:2-3). The adjusted information is classified as shown in the table below:

Table (2): Classification of Accounting Manipulation Practices

Real transactions	accounting manipulation	Nature of the form
Executing actual transactions that affect corporate accounts (e.g., advancing or delaying a transaction; or selling to customers with low credit ratings).	These manipulations exploit: The alternatives provided by legislation. The possibility of making somewhat optimistic forecasts. Legal loopholes in unregulated areas.	Legal
Actual operations not authorized under current legislation (for example, illegal transactions with companies in tax jurisdictions).	Accounting manipulations that violate regulations, for example, concealing or inflating assets, debts, sales, or expenses.	illegal

Source : Amat, O. (2019). Detecting accounting fraud before it's too late. John Wiley & Sons , page (3) .

1. Legal accounting manipulation: Publications that do not, in principle, violate accounting regulations, as they exploit the alternatives provided for in legislation, the possibility of making somewhat optimistic estimates, and legal loopholes. Many authors refer to this type of manipulation as "creative accounting," although there is no consensus, as some use this term to describe illegal accounting manipulations.

2. Illegal accounting manipulation: Practices not permitted by current legislation (hiding sales or expenses, recording fictitious sales or expenses, concealing assets or debts, etc.). Violation of current legislation can entail legal consequences, as they are accounting violation.

3. Real and legal transactions: Real and legal transactions aimed at attractively presenting the accounts. Examples include:

a. Selling real estate to achieve exceptional results promptly.

b. Selling assets and then repurchasing them to achieve results.

c. Delaying the delivery of goods to be included in the next financial year.

d. Advancing or postponing investments.

c. Increasing or decreasing expenses that are easy for the company to adjust, such as training or advertising.

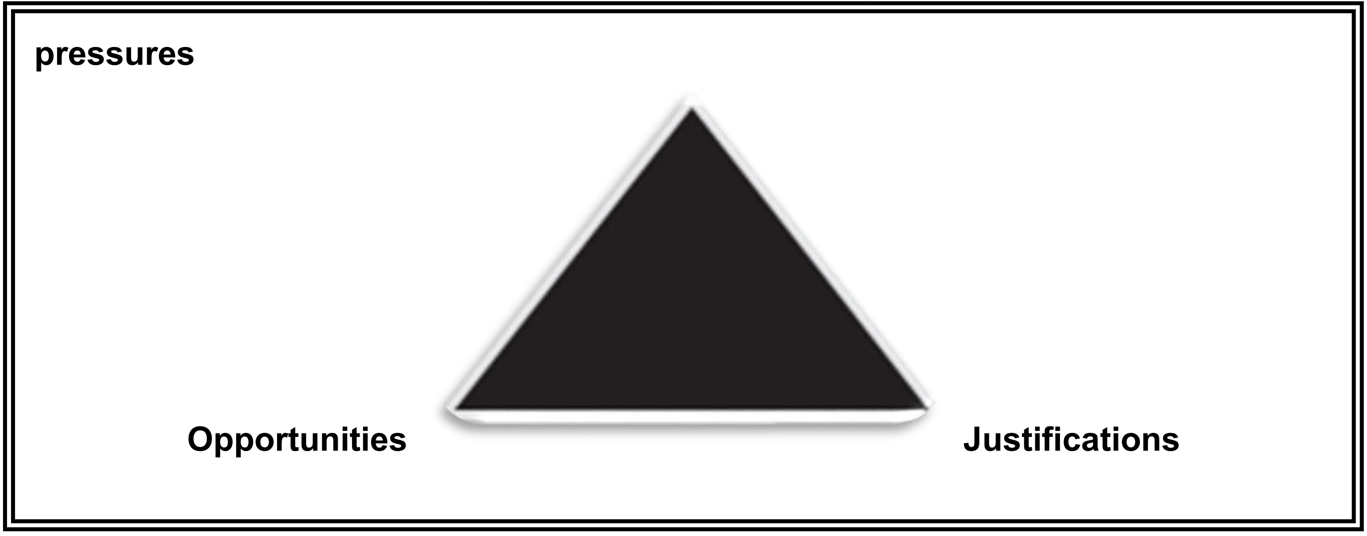
H. Issuing receipts between group companies to transfer results between them.

G. Increasing product sales to distributors (excessively increasing their warehouses) to improve results.

4. Illegal Actual Transactions: Illegal actual transactions. Examples of this include sales at prices different from market prices through offshore companies or subsidiaries in tax transactions, which impact the company's profits, assets, or liabilities.

. They harm a real person, not an anonymous computer system or an impersonal company that won't miss out on money. Fraud occurs when people have significant pressures; the opportunity to commit, conceal, and transform; and the ability to justify their personal integrity. Fraud is less likely to occur when pressures and opportunities are low, and personal integrity is high. Typically, all three elements of the fraud triangle must be present to some degree before a person commits fraud. Similarly, fraud can be prevented by removing or reducing one or more elements of the fraud triangle. While companies can reduce or mitigate some pressures and justifications, their most excellent opportunity to prevent fraud lies in reducing or minimizing the chances of it occurring by implementing and enforcing a good, effective, and robust internal control system to reduce the likelihood of an event occurring (Romney et al., 2021: 260-261).

Figure (3): Accounting fraud triangle



Source : Romney , Marshall B. , Steinbart , Paul John , Scott , L . Summers & David , A. Wood , Accounting Information Systems – Global Edition , Fifteenth Edition , Pearson Education , 2021 , page (261

2-5 Confronting the Phenomenon of Accounting Fraud by Employing Cybersecurity

Researchers believe that Cybersecurity represents the first line of defense against the phenomenon of accounting fraud in the digital age. Incorporating electronic protection tools into the design of accounting systems ensures the integrity of information, enhances the credibility of financial reports, and ultimately protects the corporate environment from the effects of financial manipulation and accounting fraud.

Third Section: The Applied Aspect

First: The Sample and Research Community

The research community comprises academics and professionals at Iraqi public and private universities and government institutions. The researchers developed a comprehensive electronic questionnaire covering all sections of the research axes. This questionnaire was distributed to a group of university professors and academics specializing in the field, as well as several employees working in government institutions who possess in-depth experience and knowledge of the research topic. This sample was carefully selected to ensure a diverse range of participants and to cover various aspects of the research topic. The number of respondents reached (77), and data was collected and analyzed to ensure the reliability and accuracy of the results. Second: Research Descriptive Data

After collecting the data resulting from the research sample members' responses to the electronic questionnaire, the researchers analyzed this data using the statistical analysis program (SPSS). Through this analysis, descriptive information was extracted, including gender, educational attainment, and scientific specialization. Table 3 shows the detailed distribution of this descriptive information.

Table (3): Demographic Information.

Percentage %	Repetition	The Details	
84.4%	65	Male	Gender
15.6%	12	Female	
5.2%	4	Diploma	Academic Specialization
14.3%	11	Bachelor's	
45.5%	35	Master's	
35.1%	27	Phd	
54.5%	42	Accounting	Scientific Specialization
13.0%	10	Business Administration	
3.9%	3	Finance And Banking	
1.3%	1	Economy	

27.3%	21	Other	
100%	77	Total research sample members	

Source: Prepared by the researchers based on the SPSS statistical analysis program.

Third: Questionnaire Reliability and Validity

The researchers used Cronbach's alpha, a type of reliability coefficient, to test the reliability and validity of the questionnaire items. Table 4 shows that the items in the first axis (cybersecurity activity) enjoyed high reliability, with a reliability coefficient of 0.866, while the reliability coefficient for the second axis (accounting fraud cases) reached 0.767. The overall reliability coefficient for all items in the research axes reached a high level of 0.843. This indicates that the questionnaire items exhibit high reliability and can be relied upon in field applications, based on the Nunnally criterion, which sets the minimum acceptable reliability coefficient at 0.70 (Sharma, 2016: 273).

Table (4): Questionnaire Reliability and Validity Coefficient

Reliability Coefficient = Square Root Of Reliability	Stability Coefficient	Number Of Paragraphs	Axis
0.930	0.866	12	Axis One (Cybersecurity Activity)
0.875	0.767	12	Axis Two (Accounting Fraud Phenomenon)
0.918	0.843	24	Total

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

Fourth: Presentation and Interpretation of the Results of the First Axis

After collecting the respondents' answers to all items in the first axis (cybersecurity activity), the researchers analyzed the answers using the statistical analysis program (SPSS). Frequencies and percentages were calculated, as well as arithmetic means and standard deviations for each item in the first axis, based on a five-point Likert scale. Table 5 shows the results of this analysis, as shown below.

Table (5): The First Axis - Cybersecurity Activity

Level	standard deviation	arithmetic mean	I totally disagree	I disagree	neutral	I agree	I totally agree	Scale	Paragraph	Survey infiltration	Order of importance
Very High	0.804	4.45	1	0.00	9	20	47	repetition	Cybersecurity is an essential component of protecting electronic financial data in Iraqi government institutions.	1	1
			1.3	0.00	11.7	26.0	61.0	Ratio %			
Very High	0.616	4.32	0.00	0.00	6	40	31	repetition	The availability of digital infrastructure enhances the	2	2

			0.00	0.00	7.8	51.9	40.3	Ratio %	effectiveness of cybersecurity in combating accounting fraud.		
Very High	0.632	4.25	0.00	0.00	8	42	27	repetitio n	Encryption is a key cybersecurity technology that protects against accounting fraud.	3	3
			0.00	0.00	10.4	54.5	35.1	Ratio %			
High	0.584	3.97	0.00	0.00	14	51	12	repetitio n	Intrusion Detection Systems (IDS) help detect accounting fraud attempts.	4	11
			0.00	0.00	18.2	55.2	15.6	Ratio %			
High	0.623	4.08	0.00	0.00	12	47	18	repetitio n	Access Control prevents unauthorized access to and hacking of accounting systems.	5	8
			0.00	0.00	15.6	61.0	23.4	Ratio %			
High	0.720	4.14	0.00	1	12	39	25	repetitio n	Modern technologies are a crucial factor in detecting fraudulent activities.	6	7
			0.00	1.3	15.6	50.6	32.5	Ratio %			
High	0.754	3.51	0.00	6	32	33	6	repetitio n	Individuals are the weakest element in the information security system in general and cybersecurity in particular.	7	12
			0.00	7.8	41.6	42.9	7.8	Ratio %			
High	0.571	4.17	0.00	0.00	7	50	20	repetitio n	Integrating processes, technologies, and people enhances	8	5

			0.00	0.00	9.1	64.9	26.0	Ratio %	the effectiveness of cybersecurity and reduces the incidence of accounting fraud.		
High	0.608	4.19	0.00	1	5	49	22	repetition	There is a direct relationship between the effectiveness of cybersecurity and the reduction of the incidence of accounting fraud.	9	4
			0.00	1.3	6.5	63.6	28.6	Ratio %			
High	0.648	4.03	0.00	1	12	48	16	repetition	توجد علاقة طردية بين فعالية الأمن السيبراني وتخفيض الإحتيال المحاسبي.	10	10
			0.00	1.3	15.6	62.3	20.8	% Ratio			
High	0.721	4.08	0.00	2	11	43	21	repetition	Integrating cyber control systems reduces the potential for financial statement fraud and asset misappropriation.	11	9
			0.00	2.6	14.3	55.8	27.3	Ratio %			
High	0.594	4.17	0.00	0.00	8	48	21	repetition	Cybersecurity activity represents the first line of defense against digital fraudulent activities.	12	6
			0.00	0.00	10.4	62.3	27.3	Ratio %			
High	0.550	4.31	1	11	136	510	266	repetition	First axis result		
			0.10	1.1	14.7	54.25	28.8	Ratio %			

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

After conducting statistical analysis on the data from the paragraphs in the first axis, which examines "cybersecurity activity," the frequencies, percentages, arithmetic means, and standard deviations were obtained for each paragraph in the first axis (cybersecurity activity). The Table above shows the order of importance for all paragraphs. The results showed that the first paragraph, which states that "cybersecurity is an essential element for protecting electronic financial data in Iraqi government institutions," ranked first in terms of average response, with an arithmetic mean of 4.45 and a standard deviation of 0.804. These results, in turn, indicate a decrease in data dispersion according to the five-point Likert scale, at a "very high" level. The results of the first paragraph indicate a strong belief among the research sample that implementing cybersecurity in Iraqi government institutions will enhance the infrastructure and technology, which in turn will preserve the confidentiality and integrity of financial data from cyber attacks. The seventh paragraph, which states, "Individuals are the weakest element in the information security system in general and cybersecurity in particular," ranked last among the paragraphs in the first axis, with an arithmetic mean of 3.51 and a standard deviation of 0.754. The response score indicates that the level of agreement was "high" according to the five-point Likert scale.

Fifth: Presentation of the results and interpretation of the second axis

To identify the opinions of the respondents regarding the paragraphs of the second axis (the phenomenon of accounting fraud), the researchers analyzed the data from the paragraphs of the second axis, attached to the electronic questionnaire, using the SPSS statistical analysis program. The results of the frequencies, percentages, arithmetic means, and standard deviations were extracted for each paragraph of the second axis based on the five-point Likert scale, which are presented in Table 6 and as shown below.

Table (6): The second axis - the phenomenon of accounting fraud

Level	standard deviation	arithmetic mean	I totally disagree	I disagree	neutral	I agree	I totally agree	Scale	Paragraph	Survey infiltration	Order of importance
High	0.823	3.92	0.00	4	17	37	19	repetition	There are instances of accounting fraud in the company you work for, which negatively impacts the quality of services provided.	1	4
			0.00	5.2	22.1	48.1	24.7	% Ratio			
High	0.902	3.77	3	3	15	44	12	repetition	The company you work for takes effective and deterrent measures to detect accounting fraud in financial records.	2	6
			3.9	3.9	19.5	57.1	15.6	% Ratio			
High	0.802	3.96	0.00	3	17	37	20	repetition	There is effective and comprehensive oversight by the	3	3

			0.00	3.9	22.1	48.1	26.0	% Ratio	internal audit teams in the company you work for to detect cases of accounting fraud.		
High	0.982	3.48	3	8	25	31	10	repetition	The company you work for uses advanced and secure technologies to detect accounting fraud.	4	12
			3.9	10.4	32.5	40.3	13.0	%النسبة			
High	0.957	3.65	4	3	20	39	11	repetition	The company you work for identifies and diagnoses the negligent and responsible parties in the event that cases of accounting fraud are discovered.	5	8
			5.2	3.9	26.0	50.6	14.3	% Ratio			
High	0.814	3.91	0.00	5	14	41	17	repetition	Weaknesses and gaps in a company's internal control systems increase the chances for managers and employees to commit financial fraud and conceal accounting fraud.	6	5
			0.00	6.5	18.2	53.2	22.1	% Ratio			
High	0.831	3.60	0.00	8	24	36	9	repetition	There are positions and justifications among company	7	10

			0.00	10.4	31.2	46.8	11.7	% Ratio	employees regarding cases of accounting fraud due to the professional pressures they are exposed to in the work environment, pressures from their subordinates, or other living and social pressures.		
High	0.836	3.53	0.00	12	17	43	5	repetition	Financial and emotional pressures on company employees can lead them to make illegal decisions and, as a result, engage in accounting fraud.	8	11
			0.00	15.6	22.1	55.8	6.5	% Ratio			
very high	0.630	4.30	0.00	0.00	7	40	30	repetition	The necessity of imposing legal and preventive measures in the company when cases of accounting fraud are discovered.	9	1
			0.00	0.00	9.1	51.9	39.0	% Ratio			
High	0.845	3.75	3	2	15	48	9	repetition	The company's management works to promote a culture that prevents the commission of accounting fraud of all kinds by adhering to the rules of professional and ethical conduct and the code of conduct.	10	7
			3.9	2.6	19.5	62.3	11.7	% Ratio			

High	0.876	3.61	3	2	26	37	9	repetition	There are programs and training courses in your company to increase employee awareness on how to recognize accounting fraud.	11	9
			3.9	2.6	33.8	48.1	11.7	% Ratio			
High	0.670	4.16	0.00	0.00	12	41	24	repetition	The importance of companies using modern technologies and employing accounting fraud examiners contributes to the early detection of accounting fraud cases.	12	2
			0.00	0.00	15.6	53.2	31.2	% Ratio			
High	0.492	4.04	16	50	209	474	175	repetition	The result of the second axis		
			1.7	5.4	22.6	51.2	18.9	% Ratio			

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

Table 6 shows the results obtained by the researchers from the paragraphs of the second axis, which study "cases of accounting fraud." Table 6 displays the frequencies, percentages, arithmetic means, and standard deviation. The results showed that paragraph nine, which states "the necessity of imposing legal and preventive measures in the company when cases of accounting fraud are discovered," ranked first among all paragraphs in the second axis, with an arithmetic mean of 4.30 and a standard deviation of 0.630. These results indicate a low degree of dispersion of respondents' responses, reflecting a "very high" agreement according to the five-point Likert scale, giving it a clear moral significance. These results indicate that the research sample members have a strong agreement that adopting such measures not only reduces the chances of fraud but also enhances the company's reputation and contributes to improving its financial stability in the long term. In contrast, the fourth paragraph, which states, "The company you work for uses advanced and secure technologies to detect accounting fraud," ranked last among the paragraphs in this axis, with an arithmetic mean of 3.48 and a standard deviation of 0.982. The response score also indicates that the level of agreement was "high" according to the five-point Likert scale.

Sixth: Analysis of the Correlation Coefficients of the Research Axes

The researchers used the Pearson Correlation Coefficient to determine the relationship between the research axes. The results extracted in Table 7 below illustrate the value of the correlation coefficient between these axes.

Table (7): Correlation Coefficients between the Research Axes

Correlations			
		First axis	The second axis
Axis 1 (Cybersecurity Activity)	Pearson Correlation	1	$.319^{**}$
	Sig. (2-tailed)		.005
	N	77	77
The second axis (the phenomenon of accounting fraud)	Pearson Correlation	$.319^{**}$	1
	Sig. (2-tailed)	.005	
	N	77	77

* Correlation is significant at the 0.01 level (2-tailed).

Source: Prepared by the researchers using the statistical analysis program (SPSS).

After analyzing the correlation coefficients for the research axes and the phenomenon in Table 7 above, we note that the type of relationship is directly proportional between the first and second axes and has moderate statistical significance at a statistical significance level less than or equal to 0.01.

Seventh: Testing the Research Hypotheses

To identify the research hypotheses, the researchers employed simple linear regression analysis (Pearson) to determine the extent to which the central hypothesis of the research was accepted or rejected. Table 7 below shows the statistical results.

Main Hypothesis:

H0: There is no statistically significant effect at a 95% confidence level between the use of cybersecurity in combating the phenomenon of accounting fraud.

H1: There is a statistically significant effect at a 95% confidence level between the use of cybersecurity in combating the phenomenon of accounting fraud.

Table (8): Analysis of variance ANOVA regression line

ANOVA^{a}						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1.872	1	1.872	8.505	.005^{b}
	Residual	16.511	75	.220		
	Total	18.383	76			

a. Dependent Variable: The second axis

b. Predictors: (Constant): First axis

Source: Prepared by the researcher using the SPSS statistical program.

Based on the results of Table (8), which relates to the analysis of variance (ANOVA), the alternative hypothesis, which states that "there is a statistically significant effect at a 95% confidence level between the use of cybersecurity in combating the phenomenon of accounting fraud," will be accepted, given that the significance value (Sig = 0.005b) is less than or equal to the significance value set by the researchers, which is (0.05). The null hypothesis, which states that "there is no statistically significant effect at a 95% confidence level between the use of cybersecurity in combating the phenomenon of accounting fraud," will be rejected.

Section Four: Conclusions and Recommendations

CONCLUSIONS

The research aims to establish the conceptual basis for employing cybersecurity as an essential policy to combat the phenomenon of accounting fraud. By testing the research hypothesis, the researchers reached a set of conclusions, as follows:

1. The researchers believe that cybersecurity represents the first line of defense against the phenomenon of accounting fraud in the digital age. Incorporating electronic protection tools into the design of accounting systems ensures the integrity of information. It enhances the credibility of financial reports, ultimately protecting the corporate environment from the effects of financial manipulation and accounting fraud.

2. Cybersecurity is a successful policy for protecting

electronic data and information in Iraqi companies. Activating cybersecurity in Iraqi government institutions will, in turn, enhance the infrastructure and technology, thus preserving the confidentiality and integrity of financial data from potential cyberattacks.

3. The importance of imposing legal and preventive measures in companies when accounting fraud is discovered. Respondents agreed that adopting such measures not only reduces the chances of fraud occurring but also enhances companies' reputations and contributes to improving their long-term financial stability.

4. There is a direct relationship between activating and adapting cybersecurity as an essential policy to protect companies' assets from attacks and threats that companies may be exposed to, including hacking, accounting fraud, and manipulation of financial statements.

Recommendations

The researchers present a set of recommendations for those interested in accounting information systems policies, including a cybersecurity policy to address negative phenomena, such as accounting fraud. The most important recommendations are the following:

1. The necessity for companies operating in the Iraqi environment to adopt contemporary methods and policies in the field of accounting information systems to protect their electronic assets. Cybersecurity is one of the most important of these policies, reducing the occurrence of negative phenomena to which these companies are exposed.

2. Companies must implement deterrent measures to prevent management and employees alike from committing negative phenomena, including accounting fraud, and to reduce the opportunities available for committing such practices. They must also ensure that no loophole is left for pressures and justifications that some may rely on to justify accounting fraud, and that a positive culture is disseminated within companies to combat this negative phenomenon.

REFERENCE

1. Razzaq, Abeer, The Role of Information Systems Oversight in Reducing Cybersecurity Risks in the Government Sector - A Field Study - Central Agency for Financial Control - Syria, a paper presented at the 14th Conference of the Arab Organization of Supreme Audit Institutions, 2024.
2. Steinbart, Paul J., and Marshall, Romney, Accounting Information Systems, Book One, translated by Qasim Ibrahim Al-Husseini, reviewed by Amin Haddad and Muhannad Atma, Mars Publishing House, Saudi Arabia, 2018.
3. Awadallah, Ahmed Hosni Saleh, The Impact of Information Security Characteristics on Achieving Institutional Excellence Through Organizational Learning Capabilities in Jordanian Universities, unpublished doctoral dissertation, submitted to the Faculty of Business Administration Council, Sudan University of Science and Technology, 2018.
4. Al-Fadl, Ali Abdul-Hussein Khalil, Amir Aqeed Kazem Al-Ardawi, and Qaisar Ali Hadi Maala, Information Technology and Databases, First Edition, University of Kufa Press, 2024.
5. Abu Al-Khair, Muhammad Haris Taha, The Impact of Internal Audit Quality on Reducing Cybersecurity Risks with the Aim of Supporting Financial Stability in Electronic Banks, a study published in the Scientific Journal of Financial and Administrative Studies and Research, Volume Fifteen, Issue One, 2023.
6. Mahrous, Ramadan Aref, and Abu Al-Hamad Mustafa Saleh, Using the Agile Methodology to Develop Internal Audit Performance to Address Cybersecurity Risks, a study published in the Journal of Financial and Commercial Research, Volume Twenty-Three, Issue Three, 2022.
7. Romney, M. B., Steinbart, P. J., Summers, S. L., & Wood, D. A. (2021). Accounting Information Systems, published 2021, Fifteenth Edition - Global Edition, © Pearson Education. Authorized adaptation from the United States edition
8. Amat, O. (2019). Detecting accounting fraud before it's too late. John Wiley & Sons
9. Arens, A. A., Elder, R. J., Beasley, M. S., & Hogan, C. E. (2020). Auditing and Assurance Services: International Perspectives. Pearson
10. Louwers, T. J., Blay, A. D., Thibodeau, J. C., Strawser, J. R., & Bagley, P. (2021). Auditing & Assurance Services. McGraw-Hill LLC
11. Margret, J. E., & Peck, G. (2014). Fraud in financial statements. Routledge
12. Haapamäki, Elina, Jukka Sihvonen, Cybersecurity in accounting research, Managerial Auditing Journal Vol. 34No. 7, 2019.
13. Khadidja, Sebkhaoui, The Role Of Cyber Security In Attending The Sustainable Development Goals, Development and Human Resources Management Review – Research and Studies Volume: 11 Issue: 01. 2024 pp:611-626.
14. Fatoki, Jacob Obafemi, The influence of cyber security on financial fraud in the Nigerian banking

industry, International Journal of Science and Research Archive, 2023, 09(02), 503–515.

15. Babiker, Iman, The Role of Internal Audit in Enhancing Cyber Security From The Auditors' Point of View, Journal of Business and Environmental Sciences, 4(1), 127-146.

16. Sharma, B. (2016). A focus on reliability in developmental research through Cronbach's Alpha among medical, dental, and paramedical professionals. Asian Pacific Journal of Health Sciences, 3(4), 271-278