International Journal of Financial Management and Economics

P-ISSN: 2617-9210
E-ISSN: 2617-9229
IJFME 2024; 7(1): 292-297
www.theeconomicsjournal.com
Received: 23-04-2024
Accepted: 28-05-2024

Khalid Aziz Farhan
College of Education for Human Sciences, University of Kirkuk, Kirkuk, Iraq

Waad Dhahir Oleiwi
College of Education for Human Sciences, University of Kirkuk, Kirkuk, Iraq

Dr. Shireen Aziz Shekhany
Department of Accounting Technical, Kirkuk Technical Institute, Northern Technical University, Iraq

Corresponding Author:
Khalid Aziz Farhan
College of Education for Human Sciences, University of Kirkuk, Kirkuk Iraq

Measuring the impact of cybersecurity risk disclosure on external audit fees

Khalid Aziz Farhan, Waad Dhahir Oleiwi and Dr. Shireen Aziz Shekhany

DOI: https://doi.org/10.33545/26179210.2024.v7.i1.304

Abstract
The study aims to measure the impact of cybersecurity risk disclosure on external audit fees by clarifying the risks of cybersecurity attacks, the importance of disclosure, and explaining the factors influencing disclosure relationships concerning cybersecurity risks and audit fees. The study population comprises companies listed on the Egyptian Stock Exchange, available for download on the website.
The Egyptian Stock Exchange represents the study population of companies listed on the exchange during the period from 2019 to 2022. The dataset includes information on the measured variables for 100 companies. It relies on financial analysis, governance reports, shareholder structure reports, board structure reports, audit committee meeting minutes, and general assembly meeting minutes. The theoretical research results have been applied, revealing several key findings, most notably a positive correlation between actual audit costs and cybersecurity breach risks. Auditors perceive an increase in cybersecurity risks, necessitating more effort in the auditing process, leading to higher audit fees.

Keywords: Cybersecurity, cybersecurity risks, external audit

Introduction
Cybersecurity concerns all business sectors, but most cybersecurity concerns in the business world focus on the financial domain. According to responses, financial information attacks will lead to negative stock market reactions, a decrease in sales growth for large companies and retailers, increased financial leverage, deteriorating financial conditions, and reduced short-term investments. Therefore, there is no doubt that financial information security is easily compromised.
In recent years, regulators and standard-setters have paid increasing attention to cybersecurity threats, reaching levels of concern studied by Rosati *et al*. (2019) [8]. The study found that in the year a company experienced a cybersecurity breach, those companies faced 28% higher audit fees compared to those that did not experience a breach. This increase was interpreted as a response to the heightened audit risk and audit efforts required.
External audits are expected as data breach risks become more complex and widespread in today's connected business environment. The rise in data breaches worldwide has raised concerns about how organizations protect their private information and maintain database integrity. This will increase professional auditors' skepticism towards corporate cyber incidents. Although companies may believe these incidents will not have a direct, quantifiable impact on financial data, significant cyber incidents will prompt auditors to make substantial efforts to investigate the incident. These investigations typically involve experts whose services revolve around addressing the cyber incident, which falls outside the scope of regular audit tasks. Consequently, predetermined audit fees will be adjusted to compensate auditors for the time and effort related to resolving the cyber incident.

Research Problem and Questions
There is a growing interest in the disclosure of internal parties in the accounting literature regarding the management of cybersecurity risks due to its clear impact on information security, company success, continuity, and quality improvement.

However, its financial reporting has not received sufficient attention from legislation and laws regarding the disclosure of cybersecurity impacts. Thus, measuring the impact of cybersecurity risk disclosure on external audit fees (Alaa, 2023) [9] remains underexplored.

The research problem is addressed by answering the following questions

1. What is meant by cybersecurity risks from the perspective of their disclosure?
2. What is the impact of disclosing cybersecurity risks on external audit fees?
3. Does the impact of disclosing cybersecurity risks differ in the absence of disclosure?
4. Is there a relationship between the disclosure of cybersecurity risks and external audit fees?

Study Objectives: The main objective of the study is to measure the impact of disclosing cybersecurity risks on external auditors' fees. This objective is achieved by explaining the risks of cyber security attacks and the importance of disclosing these risks, as well as clarifying and explaining the influencing factors. The relationship between disclosing cybersecurity risks and the fees of external auditors among companies is also examined.

Study Hypotheses

1. **Hypothesis 1:** There is a statistically significant relationship between the impact of disclosing cybersecurity risks and external audit fees.
2. **Hypothesis 2:** There is a statistically significant relationship between the impact of disclosing cybersecurity risks and the fees of external audit firms.

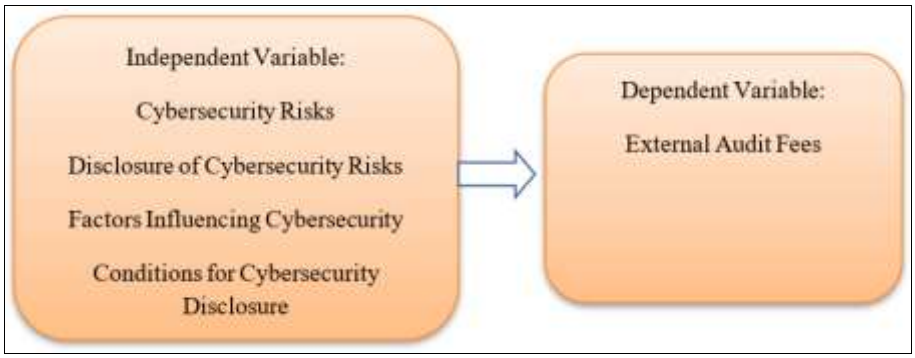

Fig 1: Study Model

Definition of Cybersecurity Risks

Cybersecurity is defined as the measures taken to protect the confidentiality, integrity, and availability of information. It encompasses a set of technologies, processes, and practices aimed at safeguarding and ensuring the protection of organizational assets. Vasarely (2017) [10] and (NSA, 2018) define cybersecurity as the regulation and allocation of resources, outlining processes and structures to protect cyberspace and other systems supporting cyber justice from cyberattacks and incidents.

In the same context, the National Cyber Security Administration (2018) emphasizes that cybersecurity comprises technologies and processes designed to protect computer systems, networks, databases, and applications, ensuring that the data they contain and the services they provide are shielded from electronic attacks, unauthorized access, modification, destruction, misuse, or unlawful exploitation. Mohammed (2020) [11] further elaborates that cybersecurity represents a collection of technologies and practices designed to protect networks, systems, computers, software, and data from attacks, piracy, or unauthorized access.

Measuring the Impact of Disclosing Cybersecurity Risks on External Audit Fees

A study referenced (Yen, J. C. *et al*., 2018) [12] suggested that this understanding might be crucial because information technology (IT) can improve the timing and accuracy of information on one hand, and reduce opportunities for control circumvention on the other. On the flip side, IT can also bring about risks related to information security.

Regarding cybersecurity risks, they are considered among the most significant risks facing a company, such as financial risks and reputation risks for companies. Cybersecurity risks can lead to increased costs and have a negative impact on revenues, weakening a company's ability to innovate, acquire, and retain customers. Electronic hacking attacks are costly and have a significant impact on a company's financial integrity.

The National Cyber Security Administration (2018) defines cybersecurity risks as threats that may include compromising a company's operations, vision, mission, management, image, reputation, or assets, as well as the possibility of unauthorized access, misuse, disclosure, destruction, alteration, or destruction of information and/or information systems.

Cybersecurity can be defined as the protection of systems, networks, software, and organizational assets from electronic attacks and incidents that may affect their effective and efficient execution of functions to achieve the goal of maintaining the confidentiality, integrity, and availability of information. This also means that companies need to increase their awareness and concern about cybersecurity risks.

In this context, the study conducted by Hansen (2022) [13] explains that audit fees at the client level are driven by the size, complexity, and various forms of risks of the client, including earnings management risks, financial risks, and corporate governance risks. Audit fees encompass all fees for audit services provided by the auditing firm, with their magnitude depending on the client company's size, the complexity of the audit process, and the audit risks. Here, there is a need for a higher level to ensure greater efforts are made to deal with higher risks.

Higher audit quality leads to the discovery of more errors, resulting in fewer audit procedures and, as mentioned in

Zhou, X's study in 2022, audit fees represent rewards. These are the necessary fees for the auditor to assess risks and complete audit work. It is necessary to assess the quality of the company's accounting information.

Audit pricing theory is defined as the basis for determining audit costs (audit fees). Auditors' fees are measured by calculating the amount using the quantity (Q) of auditor work time and computing the price (P) from the average billable rate per hour of work. Therefore, there are two perspectives in determining audit fees: the demand side and the supply side. There is a positive relationship between the demand and supply perspectives of audit fee pricing and the quality of corporate governance and audit costs. Audit fees tend to increase in response to high error risks and previously high-quality audit requests. Governance, to protect its reputation capital, experienced boards tend to focus on high-quality audit reviews by external auditors, which encourages auditors to impose higher costs.

The Relationship between Disclosing Cybersecurity Risks and External Audit Fees

Cybersecurity incidents are a concern for external auditors. Therefore, disclosing a cybersecurity incident increases the risks faced by individuals in relation to external auditors. This often leads to an increased workload in the audit process, ultimately translating into higher audit fees. Previous research by Spanos, Angelis (2017) [14], *et al*., P, Rosati; *et al*., S, K, documented the impact of cybersecurity incidents on a company's level concerning markets. This study was mentioned by Gao, L., Calderon, G.T (2021) [7].

External audit fees are influenced by the content (number of words) and language (readability) of disclosing cybersecurity risks. In terms of auditors' roles regarding cybersecurity risks, evaluating cybersecurity disclosures includes a corporate disclosure model. This means auditors need to exert greater efforts to evaluate the impact of audit risks to be able to assess cybersecurity risks. With the disclosure model, there may be a positive relationship between the number of words disclosing cybersecurity risks and audit fees. Additionally, the ease of reading the report is another advantage of disclosure, as readers can easily understand the text focusing on disclosures written in simple English language and easy readability.

As auditors face increasing scrutiny from regulatory and standard-setting bodies concerning cybersecurity, the following facts should be noted.

- External auditors pay special attention to these types of events, and they can play a crucial role in preventing or mitigating their impact by providing assurances and additional information about clients' IT controls (which represent security).
- External auditors may work with us to amend their practices, while previous cybersecurity audits continue, with additional review efforts to address security concerns.
- By providing unwavering cybersecurity for its clients, these efforts or additional measures will eventually lead to. It can also be said that the increase in audit fees means that audit fees are not predetermined.

Auditors, however, are reflective of negotiations between management and auditors. In fact, there is evidence that auditors may find it difficult to increase fees due to intense competition among audit firms. Nevertheless, regulatory bodies shed light on cybersecurity risks faced by companies, prompting pressure for compliance with cybersecurity disclosure guidelines and requests for assistance. Because auditors are better equipped to assess cybersecurity controls and identify management control issues, their expertise can assist managers in improving business preparedness for cyberattacks.

Practical Aspect

Design

- **Spatial Boundaries:** Arab Republic of Egypt.
- **Temporal Boundaries:** The questionnaire was distributed for two weeks in May 2024.

Subject Boundaries: Measuring the impact of disclosing cybersecurity risks on external audit fees.

Participants

The study community consists of companies listed on the Egyptian Stock Exchange during the period from 2019 to 2022.

Study Sample

Questionnaire Sample

The study community is represented by a random sample of companies listed on the Egyptian Stock Exchange to measure the impact of disclosing cybersecurity risks on external audit fees. The sample size is 100 companies, distributed through email, social media networks, and a list of individuals, accountants, and auditors within the companies.

Procedures

Data Collection Sources

Secondary Sources

These include books, scientific journals, publications, articles, and websites that directly or indirectly address the study topic and were heavily relied upon to enrich the theoretical framework of the study.

Primary Sources

The study methodology can be considered as the roadmap relied upon in completing the study, including the problem, significance, objectives of the study, tools used in data analysis, and the use of quantitative methods in data analysis through the questionnaire.

The study sample size was calculated based on the population size using the Richard Jigger equation.

$$n = \frac{\left(\frac{z}{d}\right)^2 \times (0.50)^2}{1 + \frac{1}{N}\left[\left(\frac{z}{d}\right)^2 \times (0.50)^2 - 1\right]}$$

Where

N: Population size.

Z: The standard score corresponding to a significance level of 0.95, equal to 1.96.

d: Margin of error.

The study sample comprised 100 individuals based on the population size.

Study Instrument Reliability

The stability of the study instrument refers to the consistency of the scale's results. To measure the stability of the study instrument (the questionnaire), Cronbach's Alpha coefficient was used to ensure its stability. Construct validity is illustrated in the following table.

Table 1: Illustrates the coefficients of the study instrument's reliability

Survey Axes	Number of Statements	Axis Stability	Axis Validity
Axis One: Disclosure of Cybersecurity Risks	7	0.910	0.909
Axis Two: External Audit	7	0.949	0.947
Overall Axis	14	0.977	0.977

The table (1) indicates the coefficients of stability for the study statements, where the total stability coefficient reached 0.977, equivalent to 97.7%. This is a high percentage, reflecting the stability of the sample results. The validity coefficients indicate the consistency of the statements and the purpose for which they were developed, with an accuracy of 97.7%, which is a very high percentage.

Statistical Description of Axes: Arithmetic Mean and Standard Deviation: Likert Scale Levels.

Table 2: Five-Point Likert Scale

Level	Weight	Arithmetic Mean
Strongly Disagree	1	From 1.00 to less than 1.80
Disagree	2	From 1.81 to less than 2.60
Neutral	3	From 2.61 to less than 3.40
Agree	4	From 3.41 to less than 4.20
Strongly Agree	5	From 4.21 to less than 5.00

From Table (3), it is shown that the response levels for the five-point Likert scale range from less than (1.80) to more than (4.21). If the arithmetic mean is less than (1.80), the response level is low on the Likert scale, and there is no impact of cybersecurity disclosure on external audit fees. If the arithmetic mean is between (2.61 - 3.40), the response level is moderate on the Likert scale, indicating some impact of cybersecurity disclosure on external audit fees. If the arithmetic mean is more than (4.20), the response level is high on the Likert scale, indicating a significant impact of cybersecurity risk disclosure on external audit fees.

Table 3: Axis One: Disclosure of Cybersecurity Risks

S. No.	Paragraph	Mean	Standard Deviation	Relative Importance	Level
1.	LEV	3.66	0.934	1	Agree
2.	LNTA	3.74	0.991	3	Agree
3.	ROA	3.94	1.023	6	Agree
4.	LNINREC	3.78	0.927	4	Agree
5.	ARL	3.71	0.957	2	Agree
6.	LOSS	3.81	0.837	5	Agree
7.	ABAFFE	3.95	0.936	7	Agree
	Overall Mean	3.71	.831		Agree

We observe from Table (3) that the sample's tendency was positive towards the paragraphs, as their overall mean indicates agreement, with the total means being greater than 3. Additionally, the table shows that the overall mean for these paragraphs reached (3.71) with a standard deviation of (0.831), reflecting agreement on the LEV. The first rank was occupied with a mean of 3.95.

Table 4: Axis Two: External Audit

S. No.	Paragraph	Mean	Standard Deviation	Relative Importance	Level
1.	Risk of Business Operations	3.84	0.861	5	Agree
2.	Size of the Entity Under Audit	3.84	0.992	6	Agree
3.	Size of the Audit Firm	3.98	0.899	1	Agree
4.	Profitability of the Audited Entity	3.78	1.031	4	Agree
5.	Complexity of Audit Operations within the Entity	3.84	0.972	3	Agree
6.	Delay in Audit Report	3.97	0.870	2	Agree
	Overall Mean	3.89	0.974		Agree

We notice from Table (4) that the survey's direction was positive because its overall mean indicates agreement, as the total mean exceeds 3.

Additionally, the table shows that the overall mean for these paragraphs reached (3.89) with a standard deviation of (0.974).

This reflects the sample's agreement on the impact of cybersecurity risk disclosure on external audit fees, as the means suggest respondents' agreement.

Results and Discussions

Summary of Results

Hypothesis Testing

Hypothesis 1: There is a statistically significant relationship

between the impact of disclosing cybersecurity risks and external audit fees.

Table 5: Correlation between Cybersecurity Risks and External Audit Fees

Correlations			
		Cybersecurity Risks	**External Audit Fees**
Cybersecurity Risks	Pearson Correlation	1	.662**
	Sig. (2-tailed)		.000
	N	100	100
External Audit Fees	Pearson Correlation	.662**	1
	Sig. (2-tailed)	.000	
	N	100	100

We observe from Table (5) that all values are positive with a significance level of ≤ 0.01, indicating a significant positive relationship between them. Therefore, the correlation coefficient is moderate. This reflects that the impact of disclosing cybersecurity risks on external audit fees has a statistically significant relationship between them.

Hypothesis 2: There is a statistically significant relationship between the impact of disclosing cybersecurity risks on external audit firms.

Table 6: Correlation Coefficient

Correlations				
		Profitability of the Audited Entity	**Complexity of External Audit**	**Cybersecurity Risks**
Profitability of the Audited Entity	Pearson Correlation	1	.682**	.687**
	Sig. (2-tailed)		.000	.000
	N	100	100	100
Complexity of External Audit	Pearson Correlation	.682**	1	.798**
	Sig. (2-tailed)	.000		.000
	N	100	100	100
Cybersecurity Risks	Pearson Correlation	.687**	.798**	1
	Sig. (2-tailed)	.000	.000	
	N	100	100	100

We notice from Table (6) that all values are positive at a significance level greater than 0.01, and there is a negative correlation between them, with a moderate correlation coefficient. This reflects the strength of the impact of disclosing cybersecurity risks on external audit firms.

Results

- Cybersecurity incidents can lead to indirect costs, including losses that are difficult to measure, such as decreased functionality, revenue, and customer confidence. This can lead to increased effort and therefore higher audit fees.
- Subsequent cybersecurity incidents occurring after the issuance of an audit report can provide external investors with negative signals about the quality of external assurance.
- Having a framework for cybersecurity risk detection provides a common language that stakeholders can use to assess a company's cybersecurity status and its risk management plan.
- There is a strong negative relationship between the cost of the external audit process and cybersecurity risks. This result aligns with many studies conducted by auditors, indicating that when more cybersecurity risks are discovered, more effort is invested in the audit process, resulting in higher audit fees.

Conclusion

The study investigated the impact of disclosing cybersecurity risks on external audit fees among companies listed on the Egyptian Stock Exchange. The research focused on understanding the correlation between cybersecurity risk disclosures and the associated audit costs.

The key findings of the study are summarized as follows:

1. **Significant Positive Relationship:** The analysis revealed a statistically significant positive relationship between the disclosure of cybersecurity risks and external audit fees. This implies that as companies disclose more information about their cybersecurity risks, the fees charged by external auditors increase. This finding is supported by the Pearson correlation coefficient of .662, indicating a moderate correlation between the two variables.
2. **Audit Effort and Complexity:** The increase in audit fees is attributed to the additional effort and complexity involved in auditing companies with higher disclosed cybersecurity risks. Auditors are required to perform more extensive procedures to evaluate and verify the cybersecurity measures and risk management practices of such companies.
3. **Impact on Audit Firms:** The study also found a significant relationship between the impact of disclosing cybersecurity risks and the fees charged by audit firms. Companies with higher cybersecurity risk disclosures tend to pay higher audit fees due to the increased complexity and time required for the audit process.
4. **Indirect Costs and Negative Signals:** Cybersecurity incidents not only lead to direct financial losses but also result in indirect costs such as decreased functionality, revenue loss, and diminished customer confidence. Additionally, cybersecurity incidents occurring post-audit can negatively affect investor perceptions of audit quality.
5. **Recommendations for Future Research:** The study suggests further research to explore multiple

dimensions of cybersecurity risk control strategies and their financial implications. It also recommends developing a comprehensive framework for cybersecurity risk detection to help stakeholders better assess a company's cybersecurity posture.

Overall, the study underscores the importance of cybersecurity risk disclosure and its significant impact on external audit fees. It highlights the need for companies to enhance their cybersecurity measures and for auditors to adapt their practices to address the evolving cybersecurity landscape.

Recommendations

- Conduct further future research to explain the relationship between multiple dimensions dependent on adaptive choices for cybersecurity risk control strategies and metrics. Financial data for IT companies contain substantial errors.
- Increase awareness of cybersecurity attack risks by providing a cybersecurity risk detection framework to enable stakeholders to assess the company's cybersecurity posture.

References

1. Sharaf IA. The impact of companies' disclosure of cybersecurity risk management report on the decisions of unprofessional Egyptian investors: An experimental study. Alexandria Journal of Accounting Research. 2023;7(1):211-281.
2. Ali MAA, Ali SAS. The impact of disclosing cybersecurity risk management report on the investment decision in the shares of companies listed on the Egyptian Stock Exchange: An experimental study. Alexandria Journal of Accounting Research. 2022;6(3):1-4.
3. Makhlouf MZH, Ghareeb HAS. Measuring the impact of disclosing cybersecurity risks on external audit fees: An empirical study. Scientific Journal of Accounting Studies. 2022;4(4):245-232.
4. Asthana S, Kalelkar R, Raman K. Does client cyber-breach have reputational consequences for the local audit office? Accounting Horizons. 2021;35(4):1-22.
5. Bao Ngo TN, Tick A. Cyber-security risks assessment by external auditors. Interdisciplinary Description of Complex Systems: INDECS. 2021;19(3):375-390.
6. Barry T, Jona J, Soderstrom N. The impact of country institutional factors on firm disclosure: Cybersecurity disclosures in Chinese cross-listed firms. Journal of Accounting and Public Policy; c2022. p. 106998.
7. Calderon TG, Gao L. Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. International Journal of Auditing. 2021;25(1):24-39.
8. Rosati F, Faria LG. Addressing the SDGs in sustainability reports: The relationship with institutional factors. Journal of cleaner production. 2019 Apr 1;215:1312-1326.
9. Fraihat BA, Ahmad AY, Alaa AA, Alhawamdeh AM, Soumadi MM, Aln'emi EA, *et al*. Evaluating technology improvement in sustainable development goals by analysing financial development and energy consumption in Jordan. International Journal of Energy Economics and Policy. 2023 Jul 9;13(4):348-355.
10. Vasarely M; c2017. www.vasarely.com/
11. Mohammed MN, Syamsudin H, Al-Zubaidi S, AKS RR, Yusuf E. Novel COVID-19 detection and diagnosis system using IOT based smart helmet. International Journal of Psychosocial Rehabilitation. 2020 Mar;24(7):2296-2303.
12. Yang CA, Li JP, Yen JC, Lai IL, Ho YC, Chen YC, *et al*. lncRNA NTT/PBOV1 axis promotes monocyte differentiation and is elevated in rheumatoid arthritis. International journal of molecular sciences. 2018 Sep 18;19(9):2806.
13. Bursch M, Mewes JM, Hansen A, Grimme S. Best-practice DFT protocols for basic molecular computational chemistry. Angewandte Chemie International Edition. 2022 Oct 17;61(42):e202205735.
14. Cappetta D, De Angelis A, Sapio L, Prezioso L, Illiano M, Quaini F, *et al*. Oxidative stress and cellular response to doxorubicin: A common factor in the complex milieu of anthracycline cardiotoxicity. Oxidative medicine and cellular longevity. 2017 Oct 18;2017.