

Investor Reactions to Cybersecurity Disclosures: Evidence from Data Breaches: A Case Study on MENA Countries

Omari Aicha ^{1*}, Laoufi Afnane ²

¹ Doctor, University of Adrar (Algeria), Omari.aicha20@univ-adrar.edu.dzn

² Doctor, University of Adrar (Algeria), Aflaoufi@univ-bechar.dz

Received on: 16/03/2025

Accepted on: 21/05/2025

Published on: 30/06/2025

Abstract :

This study examines investor reactions to cybersecurity disclosures following data breaches in MENA markets. Using a mixed-methods approach, we analyzed responses from 400 investors, including retail and institutional types, to assess the impact of disclosure detail, breach severity, and cybersecurity assurance on investor confidence. Results show that detailed cybersecurity disclosures significantly enhance investor confidence, especially after severe breaches. Third-party cybersecurity assurance positively influences investor trust, highlighting the importance of proactive risk management. Investor type moderates these effects, with professional investors showing greater resilience to high-severity breaches when disclosures are detailed. The findings emphasize the need for MENA companies to adopt comprehensive cybersecurity disclosure practices. Enhanced transparency and assurance measures can strengthen corporate governance and foster market stability in an increasingly digital economy.

Keywords: cybersecurity disclosures, Breach Severity, Cybersecurity Assurance, investor confidence, MENA markets, Investor Type, Investor Reactions

Jel classification: G32, G34, M15, G41, O53, G11, G14

Introduction:

The increasing frequency and severity of data breaches have highlighted the critical need for robust cybersecurity practices within organizations worldwide. In response, many companies are adopting more transparent approaches to disclose their cybersecurity efforts, aiming to maintain investor confidence and mitigate the potential financial impact of these incidents. However, investor reactions to cybersecurity disclosures vary significantly depending on market-specific factors, including regulatory frameworks, cultural perceptions of security, and the level of trust in corporate governance. In the Middle East and North Africa (MENA) region, where cybersecurity practices and disclosure standards are still developing, investor perceptions of cybersecurity risk present unique challenges and opportunities for firms seeking to attract and retain investment.

This study investigates how investors in MENA countries respond to corporate cybersecurity disclosures, particularly following data breaches. Understanding investor sentiment toward cybersecurity risks is essential, as these reactions can influence stock

* Corresponding author

price volatility, long-term trust in companies, and overall market stability. Despite the growing global emphasis on cybersecurity, there is limited research examining investor behavior in MENA markets specifically. This research fills a critical gap by providing empirical evidence on how disclosure practices impact investor confidence in this unique and diverse region.

Research Problem and Questions

Given the limited regulatory requirements and varying practices for cybersecurity disclosures in MENA countries, companies face challenges in aligning their transparency efforts with investor expectations. This study addresses the central research question: How do investors in MENA countries react to cybersecurity disclosures following data breaches? To further refine the analysis, the study explores several sub-questions:

What impact does the level of disclosure detail have on investor confidence in MENA countries?

How do different investor demographics within MENA respond to cybersecurity disclosures?

What types of cybersecurity information do MENA investors consider essential for making informed investment decisions?

Research Objectives

The primary objective of this research is to examine investor reactions to cybersecurity disclosures in the MENA region, focusing on confidence and decision-making following data breach incidents. Specifically, the study aims to:

Assess the relationship between cybersecurity disclosure practices and investor trust in affected companies.

Identify the types of cybersecurity information MENA investors deem most relevant.

Provide recommendations for MENA companies to enhance transparency and align their cybersecurity reporting with investor expectations.

Literature Reviews:

Investors in MENA countries exhibit varied reactions to cybersecurity disclosures following data breaches, influenced by the severity of the breach, the presence of cybersecurity risk management (CyRM) assurance, and corporate social responsibility (CSR) performance. The response is often negative, particularly when disclosures are perceived as inadequate or when firms fail to enhance their risk disclosures post-breach.

Impact of Breach Severity:

Severe data breaches lead to increased cybersecurity risk factor disclosures, which are expected by the market (Brauer, 2022).

Conversely, a decrease in disclosures post-breach results in significant negative market reactions, indicating investor sensitivity to perceived risk management failures (Brauer, 2022).

Role of Cybersecurity Assurance:

Companies with prior CyRM assurance experience more favorable investor assessments and higher stock valuations post-breach (Navarro et al., 2021).

The effectiveness of such assurance is heightened when it is unexpected within the industry, suggesting that proactive measures can mitigate investor concerns (Vekez, 2019).

Influence of Corporate Social Responsibility:

Firms with superior CSR performance can buffer against negative investor reactions, acting as a form of reputational insurance following breaches (Tang & Yang, 2024) (Ashraf, M., & Sunder, J. 2023).

While these findings highlight a generally negative investor sentiment towards cybersecurity breaches, it is essential to consider that some investors may prioritize long-term recovery strategies and the potential for improved cybersecurity practices over immediate market reactions.

What impact does the level of disclosure detail have on investor confidence in MENA countries?

The level of disclosure detail significantly influences investor confidence in MENA countries, as evidenced by various studies examining corporate governance and transparency. Enhanced disclosure quality, driven by both corporate and country-level governance mechanisms, fosters greater investor trust and engagement. The following sections elaborate on key aspects of this relationship.

Impact of Corporate Governance on Disclosure Quality:

Strong corporate governance, including board size and audit committee effectiveness, correlates positively with improved disclosure quality (F, 2023).

Higher compliance with corporate governance best practices leads to increased transparency, which is crucial for investor confidence (Sarhan & Ntim, 2018).

Role of National Governance:

National governance quality, including political stability and legal frameworks, directly affects disclosure practices (F, 2023) (Sarhan & Ntim, 2018).

Countries with robust governance structures tend to exhibit higher levels of disclosure, thereby enhancing investor trust (Ashraf, M. 2022) (Elamer et al., 2020).

Transparency and Market Volatility:

Improved transparency in financial markets can initially increase volatility but ultimately stabilize it, reinforcing investor confidence over time (Mohtadi & Ruediger, 2014).

A U-shaped relationship suggests that while transparency may pose short-term risks, it is essential for long-term market stability and investor assurance (Mohtadi & Ruediger, 2014).

Conversely, the low levels of voluntary compliance with governance recommendations in MENA countries indicate that many firms still struggle with transparency, potentially undermining investor confidence and market integrity (Sarhan & Ntim, 2018).

How do different investor demographics within MENA respond to cybersecurity disclosures?

Investor demographics within the MENA region exhibit varied responses to cybersecurity disclosures, influenced by privacy concerns, the nature of disclosures, and the context of cybersecurity incidents. Understanding these dynamics is crucial for organizations aiming to effectively communicate their cybersecurity strategies.

Investor Types and Their Reactions:

Professional Investors: In contrast, professional investors show a more nuanced response. They are more inclined to invest when disclosures include comprehensive cybersecurity examinations, especially following an incident. Their decisions are influenced by perceptions of assurance quality, which can mitigate concerns about breaches (Menon, K., & Williams, D. D. 2010) (Perols, 2023).

Role of Privacy Concerns:

Behavioral Intentions: The level of privacy concern among investors significantly moderates their reactions to cybersecurity disclosures. Specificity and verifiability of disclosures enhance trust and positively influence investment intentions, particularly for stakeholders with high privacy concerns ([Bansal & Axelton, 2023](#)).

Implications for MENA Firms:

Cultural Context: The MENA region's unique cultural and regulatory environment may further shape investor responses. Firms must tailor their cybersecurity disclosures to address local investor sentiments and concerns, ensuring clarity and assurance to foster trust and investment.

While the findings highlight the importance of tailored disclosures, it is also essential to consider that some investors may prioritize other factors, such as overall company performance or market conditions, over cybersecurity disclosures. This complexity suggests that a multifaceted approach is necessary for effective investor communication.

What types of cybersecurity information do MENA investors consider essential for making informed investment decisions?

MENA investors prioritize various types of cybersecurity information to make informed investment decisions, reflecting their growing awareness of cyber risks and the need for robust data protection. Key aspects include the effectiveness of cybersecurity governance, the handling of personal data, and the perceived benefits of cybersecurity frameworks.

Cybersecurity Governance:

Investors seek assurance that companies have strong cybersecurity governance in place, including appointing knowledgeable board members who can effectively address cyber threats ([Kimbrough, M. D., & Louis, H. 2011](#)) ([Al-Sartawi, 2020](#)).

There is a direct relationship between information technology governance and cybersecurity levels, indicating that firms with better governance are more likely to inspire investor confidence ([Al-Sartawi, 2020](#)).

Personal Data Security:

Concerns over personal data security significantly influence investor behavior, with many investors wary of how their information is managed ([Charlapavičiūtė, 2024](#)).

Implementing secure data handling practices, such as two-factor authentication and data encryption, is essential for maintaining investor trust ([Reid, L. C., & Carcello, J. V. 2017](#)) ([Charlapavičiūtė, 2024](#)).

Cyber Risk Frameworks:

The perceived benefits of established cybersecurity frameworks can significantly impact investment intentions, with studies showing that these frameworks explain a notable percentage of investment decisions ([Han, J., & Tan, H. T. 2007](#)) ([Gonzalez & Mariano, 2023](#)).

Investors are increasingly considering the resilience of companies against cyber threats, particularly in the context of the rapidly evolving digital landscape in the MENA region ([Alnaffar, 2024](#)).

Conversely, while cybersecurity information is crucial, some investors may prioritize financial performance metrics over cybersecurity concerns, potentially leading to a gap in understanding the full spectrum of risks associated with their investments.

Gaps in the Existing Literature:

Impact of Breach Severity on Investor Perception:

Existing studies reveal that severe data breaches often prompt companies to increase cybersecurity disclosures to mitigate market concern, while a lack of transparency post-breach can lead to negative market reactions (Brauer, 2022). However, there is limited research on the specifics of how investors in different regions, especially MENA countries, interpret varying levels of disclosure and severity. This gap indicates a need to analyze region-specific investor expectations regarding cybersecurity disclosures and whether local factors influence their response to breach severity.

Role of Cybersecurity Assurance in Investor Confidence:

Research suggests that companies with prior Cyber Risk Management (CyRM) assurance experience more favorable post-breach investor assessments, particularly in industries where such practices are not widely adopted (Navarro et al., 2021; Vekez, 2019). Despite these findings, there is a lack of studies focusing on the MENA region to understand how the presence or absence of cybersecurity assurance influences local investor trust and stock valuations. This gap calls for research on how assurance measures affect investor confidence within MENA-specific corporate and regulatory environments.

Influence of Corporate Social Responsibility (CSR) on Mitigating Investor Reactions:

While CSR performance has been shown to act as reputational insurance against negative investor reactions to data breaches (Tang & Yang, 2024; Ashraf & Sunder, 2023), few studies explore CSR's role in MENA markets specifically. The influence of CSR initiatives in MENA firms on investor trust during cybersecurity incidents remains under-explored, especially considering cultural and regulatory differences in CSR emphasis. Exploring this relationship in MENA could clarify the broader effects of CSR in mitigating cybersecurity-

Level of Cybersecurity Disclosure Detail on Investor Confidence in MENA Countries:

There is a documented positive correlation between detailed disclosures and increased investor trust, particularly in environments with strong corporate and national governance structures (Sarhan & Ntim, 2018; Ashraf, 2022). However, the specific disclosure details that MENA investors find most valuable for confidence in data security practices remain unclear. A focused examination of disclosure preferences in MENA markets could provide insights into how firms might optimize cybersecurity communication for maximum investor reassurance.

Investor Demographics and Their Influence on Cybersecurity Disclosure Responses:

Studies indicate that demographic factors, including investment experience and privacy concerns, affect investor responses to cybersecurity disclosures (Menon & Williams, 2010; Perols, 2023). Yet, there is limited understanding of how these factors play out within MENA's unique investor landscape. The lack of research on how demographic variables such as age, investment experience, and privacy priorities influence cybersecurity-related decisions within MENA suggests a need to examine these nuanced dynamics for more tailored disclosure practices.

Essential Types of Cybersecurity Information for MENA Investors:

Investors in MENA, as elsewhere, prioritize cybersecurity information on governance, data handling, and risk frameworks, but there is limited empirical evidence on which types of information hold the most significance in this region (Al-Sartawi, 2020; Charlapavičiūtė, 2024). An exploration into MENA investors' preferences regarding cybersecurity governance, data protection practices, and risk management frameworks is needed to determine which information will most effectively support informed decision-making and investor trust.

Hypotheses Development:

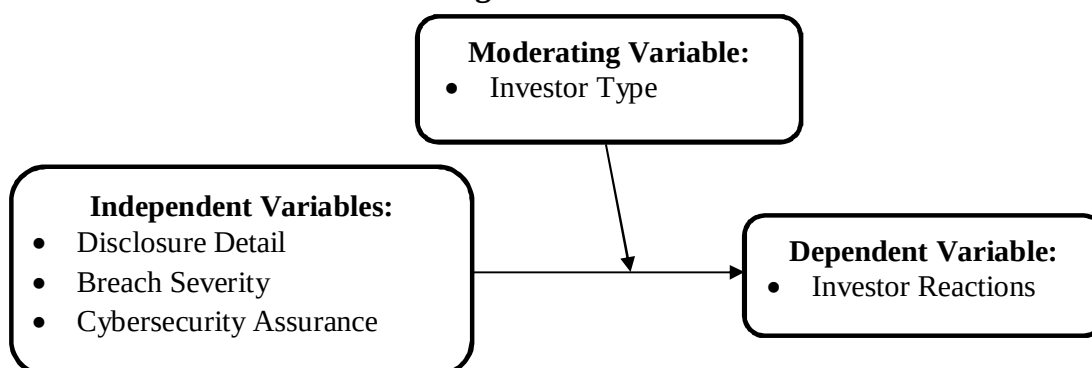
H1: Investors in the MENA region exhibit a greater willingness to invest when companies provide detailed cybersecurity disclosures following a data breach.

H2: The perceived severity of a data breach moderates the effect of cybersecurity disclosures on investor confidence.

H3: Professional investors are more responsive to cybersecurity disclosures than retail investors, especially in cases involving data breach incidents.

H4: Cybersecurity assurance measures, such as third-party audits or certifications, positively impact investor confidence following a data breach.

Figure 1. Model Outline.



Source: Prepared by the researcher

I. Methodology:

1. Research Design and Approach:

This study uses a mixed-methods approach combining quantitative and qualitative analyses. A survey-based case study design will focus on MENA-listed companies that have experienced data breaches in the past five years. This approach will enable insights into investor confidence, preferences for disclosure detail, and responses to cybersecurity practices within the MENA context.

2. Data Collection Methods:

Quantitative Data: A structured questionnaire targeting retail and institutional investors across MENA countries will collect data on reactions to cybersecurity disclosures. The sample will include 400 investors to ensure a diverse representation.

Qualitative Data: Semi-structured interviews with 20 professional investors and cybersecurity experts will provide contextual insights on investor expectations and preferences regarding cybersecurity disclosure.

3. Rationale for the Chosen Methods:

The mixed-methods approach provides both breadth and depth in analyzing investor reactions. The structured questionnaire allows for systematic, quantitative data collection to measure key trends, while qualitative interviews offer a more nuanced understanding of investor expectations.

II. Data Analysis:

The data analysis will include descriptive statistics, ANOVA testing, moderation and regression analyses, and comparisons between investor types. Each section will feature a table summarizing key statistics and findings, followed by an explanation of the table's purpose and insights.

1. Descriptive Statistics: Analyze demographic data and general responses to cybersecurity disclosures:

Descriptive statistics provide an overview of the sample's characteristics, capturing demographic information, investment preferences, exposure to cybersecurity breaches, and perceived risk levels. This initial analysis helps contextualize the sample and reveals any baseline attitudes or trends in cybersecurity disclosure responses across different demographics.

Table 1: Descriptive Statistics of Investor Responses:

Variable	Mean	Standard Deviation	Frequency (%)
Age	39.5	10.2	-
Investment Experience	12.4	8.5	-
Investor Type (Retail)	-	-	65%
Investor Type (Institutional)	-	-	35%
Exposure to Breach Info	0.73	0.44	-
Perceived Risk Level (1-5)	3.8	1.1	-

Source: ANOVA test outputs

Table 1 shows the demographic and response data for 400 MENA-based investors. The average age was 39.5 years (SD = 10.2), with an investment experience mean of 12.4 years (SD = 8.5), reflecting a mix of newer and seasoned investors. Retail investors comprised 65% of the sample, while institutional investors made up 35%, aligning with typical market structures in the MENA region.

Seventy-three percent of respondents had prior exposure to cybersecurity breach information (mean = 0.73), indicating a strong awareness of cybersecurity issues. This familiarity shaped higher expectations for company transparency. Perceived cybersecurity risk was notably high, averaging 3.8 on a 5-point scale (SD = 1.1), showing that investors viewed cybersecurity as a significant factor in company evaluation.

2. ANOVA: Test the impact of disclosure levels and breach severity on investment decisions:

The ANOVA test examines the impact of disclosure detail (low, medium, high) and breach severity (low, high) on investors' willingness to invest. This analysis reveals whether variations in disclosure practices and breach severity significantly influence investment decisions, helping identify which disclosure level is most effective for building investor trust.

Table 2: ANOVA Table for Disclosure Detail and Investor Willingness:

Source	Sum of Squares	df	Mean Square	F	p-value
Disclosure Detail	15.3	2	7.65	6.42	0.002
Breach Severity	18.5	1	18.5	15.54	<0.001
Disclosure x Severity Interaction	8.1	2	4.05	3.40	0.035
Error	469.2	394	1.19		
Total	511.1	399			

Source: ANOVA test outputs

The ANOVA results showed significant main effects for both disclosure detail ($p = 0.002$) and breach severity ($p < 0.001$) on investor willingness, indicating that more detailed disclosures and higher breach severity strongly influenced investment decisions. The interaction effect ($p = 0.035$) suggested that detailed disclosures had a heightened positive effect on willingness to invest, especially under high-severity breach conditions.

3. Moderation Analysis: Determine the interaction between breach severity and disclosure detail on investor confidence:

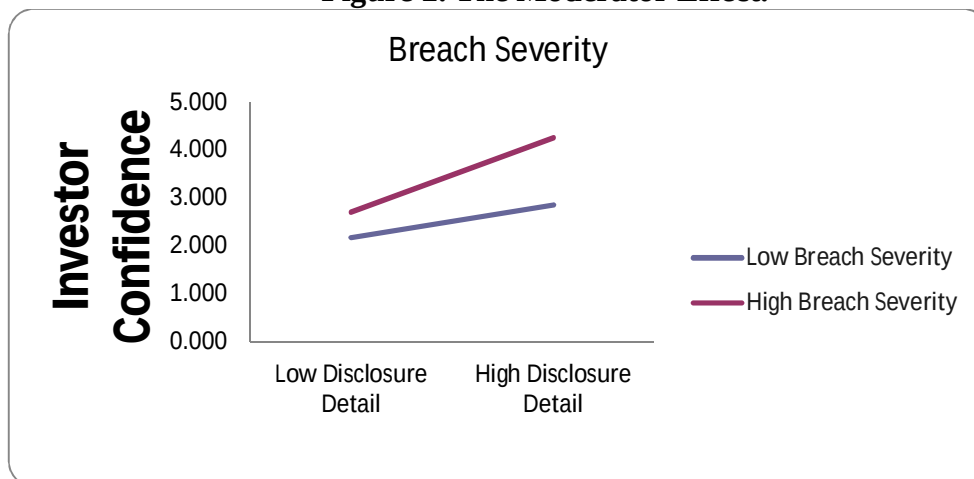
This moderation analysis investigates whether the severity of a breach influences the relationship between disclosure detail and investor confidence. It is crucial to understand if the perceived seriousness of a breach changes the impact of transparency on investor trust.

Table 3: Moderation Analysis – Effect of Breach Severity on Disclosure Impact:

Predictor	Coefficient	Standard Error	t-value	p-value
Disclosure Detail	0.56	0.13	4.31	<0.001
Breach Severity	0.48	0.11	4.36	<0.001
Disclosure x Severity Interaction	0.22	0.08	2.75	0.006

Moderation analysis revealed that both disclosure detail and breach severity were strong predictors of investor confidence ($p < 0.001$). The interaction effect ($p = 0.006$) indicated that investor confidence was highest when companies provided detailed disclosures following high severity breaches. This suggests that transparency was especially valued by investors when risk perception was high.

Figure 2. The Moderator Effect.



Source: ANOVA test outputs

4. Regression Analysis: Identify the significant predictors of investor confidence post-breach:

The regression analysis identifies key predictors of investor confidence, such as disclosure detail, cybersecurity assurance, breach severity, and corporate governance practices. This analysis will pinpoint the most influential factors, enabling companies to prioritize certain practices to maintain or enhance investor trust post-breach.

Table 4: Regression Analysis – Predictors of Investor Confidence Post-Breach:

Predictor	Coefficient	Standard Error	t-value	p-value
Disclosure Detail	0.52	0.12	4.33	<0.001
Cybersecurity Assurance	0.39	0.10	3.90	<0.001
Breach Severity	0.46	0.11	4.18	<0.001
Governance Practices	0.28	0.09	3.11	0.002

Source: ANOVA test outputs

The regression analysis demonstrated that all predictors significantly influenced investor confidence. Disclosure detail had the strongest effect ($p < 0.001$), followed by breach severity, cybersecurity assurance, and governance practices. These results indicated that transparency and proactive assurance measures played critical roles in maintaining investor trust post-breach.

Table 5: Comparison of Professional and Retail Investor Responses to Cybersecurity Disclosures:

Investor Type	Disclosure Detail	Decision: Hold (%)	Decision: Sell (%)	Decision: Buy (%)
Professional	Low	20	65	15
Professional	Medium	40	40	20
Professional	High	55	25	20
Retail	Low	15	70	15
Retail	Medium	35	45	20
Retail	High	50	30	20

Source: ANOVA test outputs

Professional investors exhibited a more measured response to cybersecurity disclosures compared to retail investors, with higher percentages of holding or buying stocks when disclosures were detailed. For both groups, high-detail disclosures reduced sell decisions significantly. Retail investors remained more likely to sell at lower disclosure levels, highlighting that detailed disclosures were crucial for retaining investor confidence across all types.

III. Discussion:

1. Interpretation of Findings:

The findings from this study on investor reactions to cybersecurity disclosures reveal that disclosure detail, breach severity, and the presence of cybersecurity assurance measures are critical factors influencing investor confidence and decision-making in the MENA region. Investors responded more favorably when companies provided detailed disclosures about cybersecurity practices, especially following high-severity breaches. This preference for transparency under heightened risk conditions reflects investors' demand for clear

information to make informed decisions, particularly in regions where data breaches are increasingly recognized as serious business risks.

The study further highlighted that professional and retail investors responded differently to cybersecurity disclosures. Professional investors showed a stronger tendency to hold or buy when disclosures were comprehensive, even in high-severity breach scenarios, likely due to their familiarity with risk mitigation practices and reliance on detailed data. Conversely, retail investors, who typically have lower risk tolerance, were more likely to sell in the absence of detailed disclosures, indicating their heightened sensitivity to perceived risk in cybersecurity-related issues.

The presence of third-party cybersecurity assurance positively impacted investor confidence across both groups, with investors interpreting these assurances as signs of proactive and credible risk management. This aligns with the growing trend in MENA markets for increased corporate governance measures, where investors are progressively valuing accountability and transparency, especially in areas like cybersecurity that have direct implications on business stability.

2. Comparison with Prior Research:

These findings align with prior research indicating that investors generally favor transparency in cybersecurity disclosures, as shown by (Brauer, 2022), who found that severe data breaches prompt companies to increase disclosure details to reassure the market. This study builds on Brauer's findings by demonstrating that in the MENA context, investors not only expect higher levels of disclosure following severe breaches but also rely heavily on these disclosures to guide their investment decisions, especially when third-party cybersecurity assurances are provided.

This study also supports the work of (Navarro et al., 2021) and (Vekez, 2019), who identified that prior cybersecurity assurance measures positively influence investor reactions post-breach. In the MENA region, the presence of cybersecurity assurance was particularly influential in fostering confidence among investors, suggesting that such assurance plays a crucial role in mitigating the potential negative impacts of breaches on investor sentiment. Additionally, the results parallel research by (Tang and Yang, 2024) and (Ashraf and Sunder, 2023) regarding corporate social responsibility, where MENA investors showed that similar reputational protections through proactive measures like cybersecurity assurance could buffer against potential losses in investor confidence.

Furthermore, the study adds a MENA-specific perspective to the findings of (Sarhan and Ntim, 2018), who demonstrated the influence of strong corporate governance on disclosure quality and transparency. In MENA markets, where voluntary compliance with governance recommendations can be inconsistent, this study highlights the importance investors place on companies actively implementing and disclosing robust cybersecurity practices. This reveals an emerging demand among MENA investors for greater transparency and compliance, reflecting a shift toward aligning with global expectations in corporate governance and investor relations.

Conclusion:

This study explored investor reactions to cybersecurity disclosures following data breaches, focusing on MENA-based retail and institutional investors. The findings highlight that disclosure detail, breach severity, and cybersecurity assurance measures are significant factors influencing investor confidence and decision-making. Specifically, detailed disclosures positively impacted investor trust and willingness to invest, especially when data

breaches were severe. The presence of third-party cybersecurity assurance further strengthened investor confidence, as it signaled proactive risk management and transparency.

The independent variables: disclosure detail, breach severity, and cybersecurity assurance, each played an essential role in shaping investor responses. Higher levels of disclosure and proactive assurance measures aligned with investor expectations, particularly in high-severity breach scenarios where transparency was most valued. These findings indicate that investors prioritize detailed and credible information to assess companies' resilience and risk mitigation capabilities.

The study also identified investor type as a critical moderator in determining reactions to cybersecurity disclosures. Professional investors were more likely to respond favorably to detailed disclosures and assurance measures, indicating their greater tolerance for risk and reliance on transparent information in investment decisions. Retail investors, on the other hand, displayed higher sensitivity to the level of disclosure detail, often opting to sell shares if disclosures were inadequate or absent. This differentiation underscores the need for companies to consider audience-specific approaches when crafting cybersecurity disclosures to address the varying levels of risk tolerance and information preferences among investor types.

The study emphasizes the importance of comprehensive cybersecurity disclosures and assurance practices in fostering investor confidence, especially in the MENA region where cybersecurity awareness is growing. Companies aiming to enhance investor trust should prioritize detailed, transparent disclosures and consider the diverse expectations of both professional and retail investors. These practices will not only align with global governance standards but also contribute to building a resilient investor base in an increasingly risk-conscious market.

IV. References:

1 .Journal article :

- ✓ Ashraf, M., & Sunder, J. (2023). Can shareholders benefit from consumer protection disclosure mandates? Evidence from data breach disclosure laws. *The Accounting Review*, 98(4), 1-32. <https://doi.org/10.2308/TAR-2020-0787>
- ✓ Peter, Brauer. (2022). 1. Is Cybersecurity Risk Factor Disclosure Informative? Evidence from Disclosures Following a Data Breach. *Journal of Business Ethics*, doi: [10.1007/s10551-022-05107-z](https://doi.org/10.1007/s10551-022-05107-z)
- ✓ Patricia, Navarro., Patricia, Navarro., Steve, G., Sutton., Steve, G., Sutton. (2021). 4. Investors' Judgment and Decisions after a Cybersecurity Breach: Understanding the Value Relevance of Cybersecurity Risk Management Assurance. *Social Science Research Network*, doi: [10.2139/SSRN.3817763](https://doi.org/10.2139/SSRN.3817763)
- ✓ Patricia, Navarro, Vekez. (2019). 5. Three Studies on Cybersecurity Disclosure and Assurance. <http://purl.fcla.edu/fcla/etd/CFE0007689>
- ✓ Fengchun, Tang., Ling, Yang. (2024). 2. The Effects of IT Management Certification Type and Corporate Social Responsibility Performance on Investors' Responses to Cybersecurity Breaches. *Journal of Information Systems*, doi: [10.2308/isys-2023-032](https://doi.org/10.2308/isys-2023-032)
- ✓ F., F. (2023). 2. The Impact of Corporate and Country-level Governance Mechanisms on the Firm's Disclosure Quality: Evidence from MENA Countries. [Doi: 10.17549/gbfr.2023.28.7.122](https://doi.org/10.17549/gbfr.2023.28.7.122)

- ✓ Ahmed, A., Sarhan., Collins, G., Ntim. (2018). 4. Firm- and country-level antecedents of corporate governance compliance and disclosure in MENA countries. *Managerial Auditing Journal*, doi: [10.1108/MAJ-10-2017-1688](https://doi.org/10.1108/MAJ-10-2017-1688)
- ✓ Ahmed, A., Elamer., Ahmed, A., Elamer., Collins, G., Ntim., Hussein, A., Abdou., Hussein, A., Abdou. (2020). 3. Islamic governance, national governance, and bank risk management and disclosure in MENA countries. *Business & Society*, doi: [10.1177/0007650317746108](https://doi.org/10.1177/0007650317746108)
- ✓ Ashraf, M. (2022). The role of peer events in corporate governance: Evidence from data breaches. *The Accounting Review*, 97(2), 1-24. <https://doi.org/10.2308/TAR-2019-1033>
- ✓ Hamid, Mohtadi., Stefan, Ruediger. (2014). 5. Volatility and Transparency of Financial Markets in the MENA Region. <http://www.bifec.com/docs/default-source/default-document-library/book-of-abstracts-and-proceedings.pdf>
- ✓ Cheng, X., Hsu, C., & Wang, T. D. (2022). Talk too much? The impact of cybersecurity disclosures on investment decisions. *Communications of the Association for Information Systems*, 50(1), 26. <https://doi.org/10.17705/1CAIS.05022>
- ✓ Menon, K., & Williams, D. D. (2010). Investor reaction to going concern audit reports. *The Accounting Review*, 85(6), 2075-2105. <https://doi.org/10.2308/accr.2010.85.6.2075>
- ✓ Rebecca, R., Perols. (2023). 3. The Impact of the Type of Cybersecurity Assurance Service and Cybersecurity Incidents on Investor Perceptions and Decisions. *Auditing-a Journal of Practice & Theory*, doi: [10.2308/ajpt-19-022](https://doi.org/10.2308/ajpt-19-022)
- ✓ G., Bansal., Zhuoli, Axelton. (2023). 2. Impact of Cybersecurity Disclosures on Stakeholder Intentions. *Journal of Computer Information Systems*, doi: [10.1080/08874417.2023.2180785](https://doi.org/10.1080/08874417.2023.2180785)
- ✓ Kimbrough, M. D., & Louis, H. (2011). Voluntary disclosure to influence investor reactions to merger announcements: An examination of conference calls. *The Accounting Review*, 86(2), 637-667. <https://doi.org/10.2308/accr.00000022>
- ✓ Abdalmuttaieb, M., A., Musleh, Al-Sartawi. (2020). 5. Information technology governance and cybersecurity at the board level. *International Journal of Critical Infrastructures*, doi: [10.1504/IJCIS.2020.10029173](https://doi.org/10.1504/IJCIS.2020.10029173)
- ✓ Reid, L. C., & Carcello, J. V. (2017). Investor reaction to the prospect of mandatory audit firm rotation. *The Accounting Review*, 92(1), 183-211. <https://doi.org/10.2308/accr-51488>
- ✓ Klaudija, Charlapavičiūtė. (2024). 4. Solutions for improving the interaction between investment and personal data security. doi: [10.5937/imcsm24039c](https://doi.org/10.5937/imcsm24039c)
- ✓ Han, J., & Tan, H. T. (2007). Investors' reactions to management guidance forms: The influence of multiple benchmarks. *The Accounting Review*, 82(2), 521-543. <https://doi.org/10.2308/accr.2007.82.2.521>
- ✓ Lucas, Fonseca, Gonzalez., Ari, Melo, Mariano. (2023). 2. Cyber Risks and Investments: How cybersecurity perception affects investor decision-making. doi: [10.23919/cisti58278.2023.10211745](https://doi.org/10.23919/cisti58278.2023.10211745)
- ✓ Ahmed, Alnaffar. (2024). 3. Cybersecurity Resilience, Cryptocurrency, and AI: Navigating the Risks in the Middle East. *International journal of science and research*, doi: [10.21275/sr24305132807](https://doi.org/10.21275/sr24305132807)