Educational Administration: Theory and Practice
2024, 30(5), 2504-2516
ISSN: 2148-2403
https://kuey.net/

Research Article

The Impact Of Cybersecurity Risk Disclosure On The Quality Of Financial Reporting And Market Value. Evidence From Egyptian Stock Market

Sameh Mohamed Amin Elnagar[1], Ahmed Said Abdel Azzim Ahmed[2], Marwa Mohamed Maher Basiouny [3*]

[1]Department of accounting, faculty of commerce, Benha university, Egypt.
[2]Department of accounting and auditing, faculty of commerce, Suez Canal university; Egypt.
[3*]Department of accounting, faculty of commerce, Benha university.

***Corresponding Author:** Marwa Mohamed Maher Basiouny
*Department of accounting and auditing, faculty of commerce, Suez Canal university; Egypt

Citation: Marwa Mohamed Maher Basiouny et al. (2024) The Impact Of Cybersecurity Risk Disclosure On The Quality Of Financial Reporting And Market Value. Evidence From Egyptian Stock Market, *Educational Administration: Theory and Practice*, *30*(5), 2504-2516. Doi: 10.53555/kuey.v30i5.3310

ARTICLE INFO

ABSTRACT

The study aims to provide evidence from the Egyptian stock market to understand the impact of cybersecurity risk disclosure on financial reporting quality and market value. The research utilizes data from nine companies in information technology, media and communications sector)IMCS) listed in Egyptian stock market spanning from 2017 to 2022 based on article (31) of the Egyptian Constitution (January 2014).The results of the study indicate that cybersecurity risk disclosure plays a crucial role in both financial reporting quality and market value, exhibiting a negative impact on financial reporting quality measures, the absolute value of discretionary accruals from the modified Jones model, and real earnings activities manipulation, higher percentage of cypersecurity risk disclosure lower portion of earning management, indicating more quality in financial reporting.The findings also highlight that a positive impact on market value represented by shares price. These results confirm the significance of transparency and trust concerning cybersecurity risks in the Egyptian stock market and demonstrate that effective management of cybersecurity risks is crucial for maintaining investor confidence, protecting firm resources, maximizing market value, sustaining long-term growth and financial position of firms.

Keywords: Cybersecurity Risk Disclosure, Quality of Financial Reporting, Market value, Egyptian Stock Market.

1. Introduction:

In the business environment, "cyber risk" describes operational disturbances that might lead to a loss of data or information's availability, confidentiality, and integrity. It may also be used to describe interruptions that can have a detrimental effect on the business operations or information technology infrastructure of a corporation. Since the majority of transactions nowadays in companies occur over the internet, wireless communication, and cloud computing, So, accounting data needs cybersecurity Protecting [1]. The financial accounting information requires robust and comprehensive security procedures. Accounting experts must be involved in discussions about business cybersecurity [2]. Information protection and the use of accounting procedures to prevent organizational, technological, public relations, and investment losses are important for cybersecurity. It is crucial to concentrate on the general concepts of protection, avoidance, and elimination of the effects of threats to the security of accounting information, regardless of the type of cyberattack [3].
cyber risk is a crucial component of operational accounting data. Such attacks cause quick client losses and increase operating expenses, which have an impact on the performance and growth of a companies and increase the risk of business [4]. it can be noted that cyber risk is taking on new horizons from the point of view of, regulators service traders, and providers, who are increasing their efforts to ensure consumer maintaining confidence and safety of the population in the market.

The nature of cybersecurity risks may vary widely and might impact business entities in many ways so, SEC 2018 put some guidance about the disclosure of these risks, it focused on that companies are recommended to review the following areas when evaluating the cybersecurity risks for disclosures: the occurrence of cyber events, the probability of potential cyber risks, the preventive measures to reduce cybersecurity threats, the cybersecurity risks of companies' operation, the costs of maintaining cybersecurity risks such as insurance coverage, the reputational damage, the costs related to existing new regulation, and 8) the litigation risks [6]
While there is growing interest in disclosure research, but there are limited studies that investigate cybersecurity risk disclosures, accounting literature recommended that managers have incentives to hold negative information [1]because disclosing bad news may reduce market value, increase cost of capital, damage future opportunities, and show information to competitors.
However, managers also have incentives to disclose negative information to reduce potential litigation cost and damage of reputation [8]. In the context of cybersecurity risk disclosure, if a company facing high cybersecurity risk fails to alarm the investors about the risk in advance and the risk materialized to an actual cybersecurity risk, the company may be exposed to lawsuits. Therefore, managers are likely to disclose cybersecurity risk if they know that the probability of future cybersecurity risks is high, and the potential implication of the risks is significant. By contrast, managers who believe that there is little chance of a cybersecurity event in the future and that the incident's impact will be minimal are less likely to reveal cybersecurity risk. Managers are unwilling to pay for the disclosure of negative data when the risk of litigation and reputational harm is low [9]. (Gordon et al., 2006) and (Wang et al., 2013) study cybersecurity risk disclosures in periods before the SEC 2005 mandate of risk factor disclosures. (Gordon et al., 2013) finds evidence of a positive effect of the Sarbanes–Oxley Act (SOX) on companies' voluntary disclosures of information security activities [10]. Wang et al. (2013) confirmed that when security risk factors involve risk-reducing action terms, companies are less likely to be associated with future attacks, proving that the nature of disclosures is important in predicting attack [11]. (Hilary et al., 2016) fail to find a significant relationship between the market reaction following cybersecurity risks and companies' prior cyber disclosures [12].
(Berkman et al., 2018) find that the market responds in a positive way to the demonstration of cybersecurity awareness in company disclosures by using a cybersecurity awareness index [13]. (Gao et al., 2020) examines cybersecurity disclosures in reports for 112 representative companies from 2007 to 2018 and find that companies' cybersecurity risk disclosures are longer when the disclosures describe a prior cyber incident [14]. where Radu and Smaili (2021) confirmed that increasing cybersecurity risk disclosure after a data breach may be saw as an ethical decision by managers [15].
Recently, national supervisors have considered cyber risk to be particularly important and have consistently assessed it due to the development of e-commerce and the Internet, a company's information assets are now some of its most valuable assets. Sadly, there is a chance that these assets will be taken, altered, or denied timely access Indeed, cybersecurity risk are capable of having a significant negative impact on the market value of a company [5],[16],[17].
Cybersecurity risk can affect the quality of financial reports. The two main characteristics that make financial statements such important for decision-making are relevance and reliability. The assumption that financial reporting is intended to provide financial information that is both relevant and accurately represents a company's current financial position based on accounting quality without information loss to stockholders and investors [18][19]. Consequently, High-quality financial statements will be impacted by low-quality financial data due to cybersecurity risks. Internal security risk due careless and incorrect handling of highly sensitive accounting data influence the reliability of financial reports [20]. This study invistigates the impact of cybersecurity risk disclosure on the quality of financial reporting and market value. Evidence from Egyptian stock market. The research uses data from (9) companies from (2017) to (2022), addressing autocorrelation and endogeneity issues. The research is organized into sections, including a literature review, data and methodology, findings and suggestions, and conclusion.

2. Review of Literature

2.1 Concept of Cybersecurity

Some definitions of cyber security were based on a set of security elements to be achieved (e.g., confidentiality, safety, availability, reliability, non-denial, certification), and the difference between definitions is that some consider that secure information is protected from all risks, while others indicate that information is secure if certain security elements (connecting security with a security package) are achieved, and although the range of security elements associated with cyber security is different, they agree on the basic elements of cyber security, namely confidentiality, safety and availability [21].
The Committee on National Security Systems ,2015 has defined the term Cybersecurity as: "Protecting information systems against unauthorized access, modifying information whether in storage, processing or transportation, or interrupting service from users, including measures to detect, document and respond to risks [6].
In the same context, the concept of cyber security from the perspective of the International Organization for Standardization (ISO), 2018) is intended to protect it from a wide range of risks to ensure business continuity, reduce business risks and maximize return on investment.

Cybersecurity also refers to science that protects information from threats to or attacks on it, whether internal or external, by providing the necessary tools and means to protect it and the standards and procedures adopted to prevent access to information by unauthorized persons [23].
Cybersecurity has become a major business concern and challenge and has therefore been careful to protect it from risks to ensure its confidentiality, integrity, availability at all stages of the life cycle of information and its use within the company [1].
The importance of cyber security represented in protecting it from risks through awareness-raising , training programmers, the application of security policy, certification, access control and encryption, also, professional bodies have given considerable attention to standards, policies, laws and regulations and their development to help business organizations secure their information against risks [24].
Because of importance of cyber security in businesses, several studies (Cisco, 2015; Ernst & Young, 2015; Pwc, 2014) have confirmed that managers and executives place the issue of cyber security at the top of their priorities and the top of their concerns to protect their companies from any external intrusions. Therefore, in the age of digitization, it has become necessary to disclose information related to cyber security in order to give more confidence and improve the mental image of the customers and related parties involved in the company, which reflecting on their competitive status and market value [27][25].

2.2 Risk Factor Disclosures

Disclosure of risk factors required in Security Act registration statements for a considerable amount of time, related to securities offerings. In 2005, the SEC mandated companies to show "the most significant factors that provide the offering harmful or uncertain" with the objective being "to provide investors with a clear summary of the material risks to an investment in the issuer's securities" [27][27]. Since companies are only required to provide qualitative descriptions and do obligate to quantify the effect of the disclosed risks, they have a great degree of freedom in what to disclose and how to disclose. Practitioners blame managers for their tendency to disclose risks wildly and to simply describe all the uncertainties they face, giving investors little information [4].
(Beatty et al., 2019) confirmed that risk factor disclosures are the easiest type of insurance to provide because, in the event of a lawsuit, "companies that cannot point to such a risk factor will wish they were able to turn back the clock and insert such language," which suggests that businesses have an incentive to provide misleading risk factor disclosures to avoid liability [23].
Recent research reduces worries that risk factor disclosures would be standardized. (Campbell et al. 2014) show that companies disclose more risk factors when facing greater risks and allocate a larger percentage of the disclosures to the description of the more serious risks [25]. Similarly, (Hope et al., 2016) show that increases in the number of risk-related words are positively related with trading volume around and after the filings, and dispersed predictions revisions around the filings. However, the effect is largely related to industrylevel risk disclosures more than firm-level disclosures [26], (Gao et al., 2020) confirmed the importance of using individual risk factors by appearing that managers add new disclosure risk factors and eliminate old risk factors on a timely basis, and such activities expect future economic changes even after controlling for ex-ante threats and company performance [22]. on the same context, there are researches mainly depends on investors' reactions to disclosed risk factors or the realization of a specific type of risks to infer the usefulness of risk factor disclosures (Nelson & Pritchard, 2016; li et al., 2018; Campbell et al. 2014) they provide direct confirmation that managers use risk factor disclosures to reflect the risks their company faces. They summarized risk factor disclosures to five categories based on the different types of risks including financial, tax, legal, systematic, and other unexpected risks. They show that the extent of risk factor disclosures about each risk type is positively connected with the extent of this type of risk measured prior to the disclosure [25][28][29].

2.3 Cybersecurity Risk Disclosure

In the light of speed and successive changes in the business environment, it has become imperative for corporations and among their recent strategic priorities, to keep pace with technological progress, respond to the strategy of the digital economy, and adapt to the ongoing change to take advantage of the areas and techniques of digital transformation [11], which has posed a challenge to professional bodies to develop the level of disclosure of corporate financial reports to include activities related to cyber security to increase confidence in their reports to enhance their competitive position and market value [30].
Due to the concerned financial, reputational, and legal impacts of recent significant cyberattacks, it is becoming more and more crucial for investors, governments, customers, vendors, and other stakeholders to be informed when making decisions about public companies' cybersecurity risks and how these risks are managed [31].
The cybersecurity risk disclosures are concerned about the risks of material cyber-attacks that the company can face. These risk disclosures should conclude specific information about the type of the risks and how each risk impacts the companies' operations. furthermore, cybersecurity risk disclosures should be coordinate with the disclosure of other functional and financial issues, the companies should evaluate the sufficiency of their disclosures of cybersecurity risks [32].
Disclosing the risks of cybersecurity risk, companies need to disclose the known important cyber threats that happened and discuss the consequences and potential costs. The risk of cyber-attacks differentiates widely.

Such threats contain several risks including but not restricted to the following: illegal access to private or sensitive data; interruption of business operations or services; expenses for necessary insurance; risk of litigation; and so on [21]. In the light of this, the United States Securities and Exchanges Authority in (SEC 2018) issued guidance to listed United States companies regarding the requirements for the optional disclosure of cyber security. It consists of two sections [6]:

Section 1: The introduction, consisting of three elements: the first, the nature of cybersecurity, addressed the definition of cyber-security, its risks to investors, companies and financial markets, the ways and objectives of cyber-incidents, the negative effects of their occurrence, the importance of disclosure to beneficiaries, and the impact on the company, its operations and its financial position.

The second element is the Cybersecurity Disclosure Guide, which began in October (2011), with emphasis on the fact that although disclosure requirements for cybersecurity risks and incidents to which the company is exposed are not mentioned in this Guide, but companies may be obliged to disclose these risks and incidents.

The third element addressed the purpose of the 2018 issue, which was to expand disclosure requirements issued in 2011 by adding two key items: first, the importance of corporate oversight policies and procedures relating to incidents and risks of cyber security, and second, the prevention of internal transactions by related parties in the event of incidents and risks related to cyber security.

Section 2: consists of two elements: first, a review of the rules on disclosure of cyber security problems represented in:

I. Relative importance: Companies must consider the importance of cyber security risks and incidents when preparing annual (10-K) and quarterly (10-Q) reports, and companies must disclose information on cyber security risks and threates in periodic reports on an adequate and continuous basis. However, if there is substantial information relating to cyber security, the model (8-K) or (6-K) should be used for immediate disclosure, thereby reducing the risk of selective disclosure.

The determination of the relative importance of cybersecurity risks or cybercrime depends on their nature, extent and potential size, but what needs to be disclosed are cyber security risks and events that are important to investors and their financial, legal or reputational implications, and take steps to prevent board members, employees and related parties from trading their securities until the investors are properly informed of the incident or the risks associated with it [33][33].

II. Risk factors: The company must disclose the risks associated with cyber security and its incidents, including the risks that arise when acquiring, and it is useful for companies to take the following factors into account when assessing the risks of cybersecurity.

- Previous incidents of cyber security, their unity and frequency.
- Potential occurrence and potential volume of cyber security incidents.
- The adequacy of the measures to reduce the risk of cybercrime and the associated costs.
- The characteristics of the company's operations that increase the incidence of fundamental cyber risks, including those of industry.
- Damage to the reputation of the company.
- Laws and regulations relating to cyber-security requirements and costs.
- The costs of organizational and judicial investigations and the resolution of cyber security incidents.

III. Financial Position and Operating Results: The company must disclose any events that could materially affect operating results and financial position, including the costs of ongoing efforts and continuous support activities specific to cybersecurity, and other costs and outcomes of potential cybersecurity incidents. Additionally, it should disclose numerous costs associated with cybersecurity issues, such as loss of intellectual property rights, competitive position loss, costs of preventative measures, insurance, regulatory and legal investigations, and preparations for current or proposed legislation.

IV. Nature of Business Description: The Company must disclose incidents or cybersecurity risks that could materially impact products, relationships with customers, suppliers, or competitive position.

V. Legal Proceedings The company must disclose information related to material pending litigation concerning cybersecurity issues, whether for the parent company or subsidiaries. For example, if the company experiences customer data theft resulting in lawsuits against the company, details of the lawsuit must be disclosed, including the name of the court handling the lawsuit, hearing dates, key parties to the case, and claims.

VI. Disclosure in Financial Statements Cybersecurity incidents and the risks associated with them may affect a company's financial statements, leading to:

- Increased expenses related to investigation, breach notification, remediation, and potential litigation, along with costs for legal and other professional services.
- Decreased revenues, as companies may need to offer additional incentives to retain customers or risk losing them.
- Warranty claims, contract breaches, product recalls/replacements, third-party liabilities, and increased insurance premiums.
- Decreased future cash flows or impairment of intangible assets, along with recognition of additional liabilities and increased financing costs.

- The company must disclose the role of the board of directors in managing cybersecurity risks and its risk management program in collaboration with company management, which positively impacts investors by fulfilling the board's role in these important matters. Therefore, companies must design a financial reporting and control system for disclosing cybersecurity to ensure that information regarding the scope and magnitude of the financial impacts of cybersecurity incidents is considered when preparing financial statements in a timely manner.

Section (2) concerning policies and procedures, it included the following items:

I. Disclosure of Control Measures: Companies must consider whether the controls and procedures related to disclosure enable appropriate disclosure of information regarding cybersecurity risks and incidents [34]. These measures should help identify cybersecurity risks and incidents, assess and analyze their impact on company operations, and facilitate open communication channels between disclosure experts and technicians. The CEO and CFO must ensure the design and effectiveness of disclosure controls and procedures and disclose a summary of the adequacy and effectiveness of these controls and procedures, ensuring no deficiencies that render them ineffective [35][35].

II. Insider Trading Companies: the directors, employees, and other related parties must comply with laws regarding insider trading concerning undisclosed information about cybersecurity risks and incidents, including vulnerabilities and breaches [36][36]. Trading based on undisclosed material information violates trust and loyalty to the company, its shareholders, and the laws and trading rules in force while holding such undisclosed information [15]. Companies must have well-designed policies and procedures to prevent trading of all types of undisclosed material information, including information related to cybersecurity risks and incidents. Insider trading is prohibited during investigations into material cybersecurity incidents and before disclosure, taking precautionary measures [37][37].

III. Regulations and Selective Disclosure: Companies must have procedures to ensure nonselective disclosure of information related to cybersecurity risks and incidents before disclosing the same information to the public [38]. in this study we apply in Egypt so we will discuss the Egyptian's efforts in supporting cybersecurity:

the Egyptian Constitution issued Article 31 (January 2014) stipulates that "cyberspace security is an integral part of the national security system, and the state is committed to taking necessary measures to preserve it as regulated by law." Accordingly, the National Cybersecurity Strategy (2017-2021) was developed, aiming to confront cyber risks, enhance trust in communication and information infrastructure, applications, and services across vital sectors, ensuring a secure and reliable digital environment for the Egyptian society. The strategy includes:

- Challenges and Cyber Threats: such as infrastructure penetration and sabotage, cyber warfare terrorism, digital identity theft, and data theft.
- Targeted Vital Sectors: including communications and information technology, energy, government services, transportation, health, emergency services, media and culture, official state websites, and sectors influencing economic activity like commerce, industry, agriculture, irrigation, education at all levels, investment, and tourism.
- Key Elements of Cyber Threat Severity: based on advanced and evolving techniques, rapid and widespread dissemination, and broad impact.
- Strategic Preparedness/Direction to Address Cyber Threats: political, institutional, strategic, legislative, regulatory, research and development, human resource development, and cooperation with friendly countries, international and regional organizations, and community awareness.
- Implementation Mechanism: through the formation of the Supreme Cybersecurity Council to protect communication and information technology infrastructure under the supervision of the Ministry of Communications and Information Technology, chaired by the Minister of Communications. The council oversees the development and implementation of a national cybersecurity strategy, subject to updating in light of successive technological developments.
- Key Strategic Programs in the Current Phase (2017-2021): include developing suitable legislative frameworks for cybersecurity, combating cybercrime, protecting privacy, and digital identity, developing a comprehensive national system to protect cyberspace security and secure communication and information technology infrastructure, and activating the necessary infrastructure to support trust in electronic transactions in general and electronic government services. Additionally, a law combating cybercrimes, commonly known as combating internet crimes, has been issued.

This comprehensive approach reflects Egypt's commitment to cybersecurity and its efforts to protect its digital infrastructure and ensure a safe digital environment for its citizens.

2.4 Cybersecurity Risks Disclosure and Quality of Financial Reporting

Cybersecurity risks have implications for the quality of financial reporting [20]. Financial analysts consider cybersecurity information in their investment analysis process, looking at company strategy, integration of cybersecurity, and certification of cybersecurity information. They find boilerplate or cursory cybersecurity information in financial reports to be unreliable and prefer other information sources [39]. Maintaining accurate and dependable financial data is fundamental, but internal and external risks threaten the confidentiality, integrity, and availability of this data [2]. Cybersecurity potentially has an impact on financial

reporting quality, which is one of the duties of audit committees [1]. Cybersecurity risks that could impact the accuracy and reliability of financial quality reports include internal and external threats to the confidentiality, integrity, and availability of financial data [40]. These risks can range from viruses to hacktivists, ransomware, and denial-of-service attacks. The interconnection and usage of electronic data gathering, storage, and transfer increase the likelihood of cybertheft, damage, or disruption [38]. Information leakage poses a threat to financial institutions, affecting their ability to operate properly and generate financial returns [41]. Cybersecurity incidents can also signal internal control weaknesses and pose risks to the quality of financial reporting [42]. Cybersecurity is a risk that extends to all operations of companies and potentially impacts financial reporting quality, making it a concern for audit committees.

Cybersecurity risks significantly impact financial quality reports, as they can compromise the integrity of financial data, leading to inaccuracies in financial statements [34],[21]. Companies experiencing cybersecurity breaches may face legal and reputational risks, which can negatively affect financial quality reports and investor perceptions. Compliance with disclosure requirements by regulatory bodies like the Securities and Exchange Commission (SEC) can result in legal and reputational risks, impacting financial quality reports and investor perceptions [41][42]. Cybersecurity incidents can damage a company's reputation and brand value, affecting financial performance. Financial quality reports may reflect these adverse effects through indicators such as declining revenues, increased customer complaints, or higher marketing expenses required to repair the brand image[34],[2]. Compliance costs and operational impact can also be significant for companies, as addressing cybersecurity risks and complying with regulatory requirements can incur significant costs. These costs may increase operating expenses and reduce profit margins, while disruptions can lead to revenue losses, productivity declines, and additional expenses associated with incident response and remediation efforts. Litigation and legal expenses from cybersecurity breaches can result in substantial legal expenses, settlements, or judgments that impact financial performance. Insurance coverage and financial resilience can also be affected by cybersecurity risks, as insurers may impose limitations or exclusions based on a company's cybersecurity practices [2][21].

Credit ratings and financing costs can also be impacted by cybersecurity risks, as credit rating agencies consider factors such as cybersecurity preparedness, incident response capabilities, and potential financial impact of breaches when assessing a company's credit risk. Financial quality reports may reflect supply chain risks, vendor management practices, and contingency planning efforts to mitigate potential disruptions. Regulatory enforcement and penalties can result from non-compliance with cybersecurity regulations or failure to adequately protect customer data. This proactive approach can enhance investor confidence, preserve shareholder value, and strengthen a company's resilience in the face of evolving cyber threats [20][43].

Based on the previous presentation, the hypothesis can be formulated as follows:

H1: There is a significant relationship between cybersecurity risks Disclosure and Quality of Financial reporting.

2.5 Cybersecurity Risks Disclosure and Companies' Market Value

The relationship between cybersecurity risks and companies' market value is complex and multifaceted. Cybersecurity risks can arise from various sources such as cyberattacks, data breaches, malware, insider threats, and inadequate security measures. These risks can have a significant impact on a company's market value through various factors. Financially, cybersecurity incidents can result in financial losses, affecting investors' perceptions of the company's future earnings and growth prospects [34]. Additionally, a company's reputation for maintaining strong cybersecurity measures can enhance trust among stakeholders, while high-profile breaches or a perceived lack of preparedness can damage reputation and erode trust, leading to a decrease in market value [44]. Non-compliance with cybersecurity regulations and standards can expose companies to legal and regulatory risks, negatively impacting market valuation [4]. Investor perception is also influenced by cybersecurity, with companies demonstrating robust cybersecurity practices being viewed more favorably, leading to higher market valuation [9]. Operational resilience is crucial, as companies that effectively respond to and recover from cyber threats can mitigate negative impacts on market value [3]. Overall, effective management of cybersecurity risks is essential for maintaining investor confidence, protecting market value, and sustaining long-term growth.

Cybersecurity risks have a significant impact on companies' market value. Cyber terrorist attacks on companies lead to a decline in stock prices, damaging the market valuation of the firm [45]. Companies that experience cyberattacks suffer financial and reputational losses in the market [43]. Cybersecurity breaches can also affect brand value, market value, and overall corporate reputation [30]. The long-run abnormal returns of firms following security breaches can influence their market value [46]. The adverse impact and risk of hacking events on firms' market valuations are evident, highlighting the need for robust regulatory mechanisms for prevention and enforcement of data security breaches [47].

Cybersecurity risks significantly impact a company's market value. Financial losses, reputational damage, regulatory compliance, investor perception, and operational resilience are all factors that influence this relationship. Financial losses can lead to a company's future earnings and growth prospects, affecting its market value. A company's reputation can enhance trust among customers, investors, and stakeholders, while non-compliance can expose it to legal risks [48]. Non-compliance can signal weaknesses in governance and risk management practices, negatively impacting market valuation. Investors increasingly consider

cybersecurity as a material risk factor, leading to higher market valuation for companies with robust cybersecurity practice. Operational resilience can mitigate the negative impact of cyber threats, while poor response capabilities may lead to significant valuation declines [49]. Effective management of cybersecurity risks is crucial for maintaining investor confidence, protecting market value, and sustaining long-term growth. Based on the previous presentation, the hypothesis can be formulated as follows:
H2: There is a significant relationship between cybersecurity risks disclosure and companies' market value.

3. Research Design and Methodology

3.1 Data Collection and Sample Selection Database

The data of the study refers to (10) companies in information technology, media and Communications sector)IMCS) listed in Egyptian stock market (the study excluding DIGITIZ company which established 2021). The study choose the period (2017 : 2022) based on article (31) of the Egyptian Constitution (January 2014) states that: "The security of information space is an essential part of the national security system and the State is obliged to take the necessary measures to preserve it as regulated by law." Accordingly, the National Cybersecurity Strategy (2017-2021) was developed, the strategic objective of which is to address cyber-risks and to promote confidence in the communications and information infrastructure, applications and services in various vital sectors and to ensure a secure and reliable digital environment for Egyptian society in its various sectors. The final number of observations is (216= 9*6 *4) for the analysis of this study. The collection of applied study data has relied on Internet sites where financial statements for Egyptian listed companies are available.
These sites include: http://www.mubasher.info/EGX/listed-companies www.egx.com.eg http://www.hcestox.com/companies.aspx

3.2 Measurement of Variables:

The independent variables in the study are:

Cybersecurity Risk Disclosure (CRD): cybersecurity risk disclosure in the financial reports concerning information security allow a company to give signals to the market that the company is actively engaged in, detecting, decreasing and correcting security risks. These signals should increase a company's share price in the exchange stock market in many ways. these signals also, increase shareholder' trust to get in ecommerce by mitigating the un-confidence of practicing business online that is associated with information security concerns [11]. An increase in shareholders' trust and investors should increase the company's expected net cash flows and, the firm's market value. So, in our study (**CRD)** can be measured through a dummy variable that equals (1) if the company disclose its cyber risks in financial reports and (0) otherwise.

The dependent variable represented by

1- Quality of Financial reporting (QFR): There are two main types of quality of financial reporting measures in related accounting literature, there is considerable variation in the variable estimations and measurement. Inspired by (Dou et al., 2018) and (Hope et al, 2020), First method , we use (**AVDA)**, the absolute value of discretionary accruals from the modified Jones model (Dechow et al., 1995), Second method , we measure firms 'QFR with real earnings activities manipulation **(REM**) related to abnormal discretionary expenses, production costs, and operating cash flows following studies [26][50].

2- Market value (MV): Market value (MV) for a company is the price per share multiplied by the number of shares outstanding. because companies have up to 90 days to "officially "end the annual filings with the Egyptian stock market (EGX), the study used a three-month lead price. This lead price is vital in our research model because the disclosure of cybersecurity risks) are provided in the EGX annual reports. Accordingly, if there were any effect of the voluntary disclosures regarding cybersecurity risks, we needed to select a time when this information was provided to the investors. Therefore, SP_{it} is the share price of the company three months after the fiscal year-end. Since the data includes the year 2017, we used quarterly database (Q1) 2018 to get P_t+Q1 prices for all companies, Furthermore, the study restricted sample to companies with a fiscal yearend of December.
The research model used in our study is a modified version of the model by Ohlson (1995). This model has been used in the literature and is shown in equation (1) below:

$$SP_{it} = \beta 0 \times Intercept + \beta 1 \times Disc_{it} + \beta 2 \times BVPS_{it} + \beta 3 \times EPS_{it} + \beta 4 \times LnASS_{it} + \beta 5 \times NEG_{it} + \sum \beta_k \times Year_{it} + \sum \beta_j \times Indus_{it} + \varepsilon_{it}$$

where:
SP_{it} = Stock price of company i for year t, 90 days after fiscal year close
$Disc_{it}$ = Proxy variable for voluntary disclosure concerning cybersecurity. The study estimates two regression specifications as follows:
1) Base model without any disclosure variable
2) voluntary Cypersecurity disclosure, where Disc = 1 if any disclosure concerning cybersecurity, zero otherwise
EPS_{it} = Earnings per share (basic excluding special items) for firm i for year t, year-end $BVPS_{it}$ = Book value of equity divided by number of shares outstanding for firm i for year t, year-end

$LogAss_{it}$ = Log of total assets of firm i for year t
NEG_{it} = 1 if EPS is negative for firm i for year t, zero otherwise Year = 1 if current year, zero otherwise
Indus = 1 if firm is in a particular industry, zero otherwise

Control variables in this study shown as follow:

- Sales growth rate (SGR): sales for the company i in the year t– sales for the company i for the year t-1 divided by sales for the company i for the year t-1.
- Institutional shareholding (INSHOLD): Percentage of shares held by institutions for firm i for year t over total shares outstanding.
- Return on assets (ROA): Net Income divided by Total Assets
- Market to Book value (MTB): dividing the current closing price of the stock by the book value per share.
- Stock Return (RETURN): Annual Stock Return

Institutional Share INSHO Percentage of Shares Held bHolding LD Institutions for Firm i for Year Over Total Shares Outstanding oo

3.3. Estimation Method and Models

Table 2 presents the summary of variables.

Type	Variable	Name	Symbol	Measurement Method
Independent Variable	Cybersecurity Risk Disclosure	Cybersecurity Risk Disclosure	CRD	Dummy Variable (1 or 0)
Dependent Variable	Quality of Financial Reporting	Discretionary Accruals	AVDA	Modified Jones Model (MJM)
		Real Earnings Management	REM	Abnormal Discretionar Expenses, Production Costs, an Operating Cash Flows
	market value	Stock Price	SP	Modified Version of the Model b Ohlson
Control Variables		Sales Growth Rate	SGR	$sales_{it} - sales_{it-1}/sales_{it-1}$
returns on Assets	ROA	Net Income/ Total Assets		
Market to Book value	MTB	Dividing the Current Closin Price of the Stock by the B Value per Share		
Stock Return	RETURN	Annual Stock Return		

The present study uses multiple regression models to clarify the Impact of cybersecurity risk disclosure on the quality of financial reporting and market Equations (1) used to investigate the impact of cybersecurity risk disclosure on the quality of financial reporting At the same time, Equation (2) indicates the impact cybersecurity risk disclosure on market value .The present study uses two equations for the (9) samples with (216) total observations collected. To Investigate the effect of cybersecurity risk disclosure on the quality of financial reporting and market in companies of information technology, media and Communications sector)IMCS) listed in Egyptian stock market.
To test our H1, we run the regression of the event of company's disclosure of cyber security risks (CRDi,t) on quality of financial reporting (QFRi,t) We expect disclosure of cybersecurity risks will increase the quality of financial reporting. Thus, we predict that the coefficient =β o is significant

$$QFRi,t = \beta o + \beta_1 CRDi,t + \beta_2 SGRi,t + \beta_3 INSHOLDi,t + \beta_4 ROAi,t + \beta_5 MTBi,t + \beta_6 RETURNi,t + \sum i,t \quad (1)$$

CRDi,t is a dummy variable that equals 1 if the company discloses its cyber risks in that quarter and o otherwise.
To test H2, we run the regression of company's disclosure of cyber security risks (CRDi,t) on market value (MVi,t).

$$MVi,t = \beta o + \beta_1 CRDi,t + \beta_2 SGRi,t + \beta_3 INSHOLDi,t + \beta_4 ROAi,t + \beta 5 MTBi,t + \beta_6 RETURNi,t + \sum i,t \quad (2)$$

The symbol βo denotes the constant value, and the symbol ∑ indicates the error term.

4. Analysis and Results:

4.1 Descriptive Statistics

The mean value of (AVDA) and (REM) is (0.1834) and (0.2650) with a standard deviation of (0.2916) and (0.3021), respectively, which shows that (AVDA) and REM has a simple variation between each other the standard deviation of (SP) is (0.1049)

4.2 Correlation analysis

Correlation analysis results are shown in Table 5. In terms of cybersecurity risk disclosure is negatively with quality of financial reporting (AVDA , REM), this is due to the fact that a higher percentage of disclosure about

related risk of cybersecurity indicates that a smaller portion of earning management through discretional and real activities manipulation which means more quality in financial reporting and more accurate information . This Results agree with [20][34][39].
On the other hand, the relationship between (CRD) variable and market value (SP) is positive and significant Which means cybersecurity risk may having a significant negative impact on the market value of a company but the more disclosure about these risks has a positive impact on shares price and market value of the companies. this result agree with [4][9][30][43].
The correlation shows that (INSHOLD) is signifcant positively correlated with CRD this result indicate that institutions shareholding could help decreasing agency problems and concern about the company's long-term development. When firms have higher institution shareholding and less agency problems, they are more incentivized to increase disclosure about cyper security risk and increase FRQ through decresing their measures in our study (AVDA,REM). The correlation also shows that CRD has a significant positive relationship with MTB This is because companies which disclose about cypersecurity risk in their reports increase the transparency and increase the investores trust about financial performance for these companies which in return increase market value of shares.

4.3 Regression analysis

Table (5 and 6) represented the result of regression analysis for the models of the present study. Tables include all independent, control variable coefficients, t-statistics, standard error and probability values. Additionally, tables have the values of R-Square , adjusted R-Square and Wald Chi-square. results from both the AVDA and REM models are reported. It is observed that cypersecurity risk disclosure have a negative effect on both AVDA and REM which is consistent with the a priori hyposiyes which means more quality of financial reporting.on the other hand ,it is observed that cypersecurit risk disclosure have a positive effect on shares price which represent market value in our study colume (4) and (7) in table 1 show that The value of significance level is less than (0.05), Therefore, it has a significant impact, as it is clear to us that the sign of the regression coefficient (β) is negative, and this means that there is a negative significant and statistically correlation between cypersecurity risk disclosure (CRD) and quality of financial reporting measures (AVDA, REM) consistent with the results of the study [20][34][39] Which means that this kind of disclosure about risks related to cypersecurity , reduces earning management practices in companies which confirm that companies care about the quality of reports and it is an important topic for the media and communication sector in egyptian exchange market . The reason for the negative effect can be attributed to highinterest rates set by managers to increase confidence and have the trust of investores and relaties parties .in colume (4) in table(6) show that The value of significance level is less than (0.05), Therefore, it has a significant effect as it is mention that the sign of the regression coefficient (β) is positive, which means that there is a positive significant and statistically correlation between cypersecurity risk disclosure (CRD) and markt value represnted in stock price consistent with the results of the study [4][9][30][43].
This result indicates that cyber risk is an important matter of operational accounting data. Such risks can cause investors losses and increased operating expenses, which have an impact on the performance and growth of a companies. in recent days a company's information assets are one most valuable asset. so, there is a chance that these assets will be taken, by cyber-attacks so disclosure about it having a good impact on investors and increase their trust about the financial positions of companies which increase its market value.
The value of the R- Square was (0.425) , (0.403) and (0.362) respectively. This value indicates that the independent variable in the model, cypersecurity risk disclosure (CRD), explains (42.5%) ,(40.3) and (36.2%) respectivly of the change in the dependent variable, quality of financial reporting (AVDA,REM) and market value (MV) .

Table 3. Descriptive statistic

AVDA	0.1834	0.2743	0.0020	0.5342	0.2916
REM	0.2650	0.1502	0.0010	0.3671	0.3021
SP	0.1047	0.0916	-0.4802	0.2943	0.1049
SGR	0.2190	0.1853	-0.3571	0.4160	0.2105
INSHOLD	12.4821	11.9840	0.3656	18.3765	23.8430
ROA	0.0326	0.0265	-0.1242	0.1917	0.0529
MTB	1.0514	1.0049	0.7531	6.5832	1.0951
RETURN	0.1732	0.0128	-0.5683	3.1654	0.8097

Variable Mean Median Minimum Maximum Standard Deviation

Table 4. Correlation analysis of variables

Variable	CRD	AVDA	REM	SP	SGR	INSHOLD	ROA	MTB	RETURN
CRD	**1.000**								
AVDA	**-0.019****	**1.000**							

REM	**-0.047****	**0.025****	**1.000**						
SP	**0.038****	**0.590**	**0.230**	**1.000**					
SGR	**0.069**	**0.760**	**0.085**	**0.047****	**1.000**				
INSHOLD	**0.014****	**-0.016****	**-0.021***	**0.018****	**0.007***	**1.000**			
ROA	**0.084**	**-0.007***	**-0.018****	**0.013****	**0.024****	**0.037****	**1.000**		
MTB	**0.009***	**0.603**	**0.159**	**0.040****	**0.091**	**0.006***	**0.005***	**1.000**	
RETURN	**0.081**	**-0.049****	**-0.007***	**0.153**	**0.003***	**0.023****	**0.042****	**0.081**	**1.000**

Note: ** Correlation is significant at the p = 0.05, * Correlation is significant at the p = 0.01 level. Data are rounded off to the fourth decimal.

QFR (AVDA) QFR (REM)

Table 5. Variable regression analysis

	Coeffficient	Std.Error	Prob.	Coeffficient	Std.Error	Prob.
Constant	-0.06407	0.00626	0.00001	-0.00823	0.00840	0.00435
CRD	-0.01063	0.00085	0.03047**	-0.04366	0.00215	0.02068**
SGR	0.05785	0.05826	0.06394	0.00587	0.00587	0.07104
INSHOLD	-0.03047	0.00058	0.04139**	-0.00629	0.00646	0.00963*
ROA	-0.00427	0.00439	0.00025*	-0.05685	0.00812	0.03801**
MTB	0.02036	0.06403	0.08076	0.00645	0.00648	0.06413
RETURN	-0.04039	0.00078	0.01503**	-0.04710	0.04723	0.00728*
R- Sqare		0.425		R- Sqare		0.403
Adjusted R-Square		0.417		Adjusted R-Square		0.395
Wald Chi-square		11.01		Wald Chi-square		13.17
Prob.		0.000		Prob.		0.000

Variable Note: *, **, mean significant at 1 % and 5 %..

Table 6. Variable regression analysis

Variable	MV		
	Coeffficient	Std.Error	Prob.
Constant	0.04315	0.00029	0.00004
CRD	0.06197	0.00146	0.01409**
SGR	0.01027	0.00237	0.03821**
INSHOLD	0.02613	0.06942	0.01567**
ROA	0.01008	0.00638	0.02368**
MTB	0.05410	0.01026	0.04310**
RETURN	0.06825	0.01739	0.09163
R- Sqare		0.362	
Adjusted R-Square		0.357	
Wald Chi-square		9.05	
Prob.		0.000	

5. Conclusions and Recommendations:

This study Investigated the impact of cybersecurity risk disclosure on the quality of financial reporting and market value in Egyptian stock market. This study applied on (9) companies in information technology, media and Communications sector (IMCS) listed in Egyptian stock market.

The study showed that cypersecurity risk disclosure (CRD) has a negative effect on real earnings activities manipulation (REM) and the absolute value of discretionary accruals from the modified Jones model (AVDA) which used to measure the quality of financial reporting (QRF) , this means a higher percentage of disclosure about related risk of cybersecurity a smaller portion of earning management indicating more quality in financial reporting (positive impact on quality of financial reports).

The study showed also a positive significant and statistically relationship between cypersecurity risk disclosure (CRD) and markt value represnted in stock price.
Regarding control variables of the study (INSHOLD) is signifcant positively correlated with (CRD) this confirm that institutions shareholding help in decreasing agency problems and concern about the company's going concern. When companies have higher institution shareholding and less agency problems, they are more interested to increase disclosure about cyper security risk and increase (FRQ) through decreasing (AVDA,REM) also, (CRD) has a significant positive relationship with(MTB) because firms which disclose information about cypersecurity risk in reports increase the transparency and investors trust about financial performance for them which in return increase market value of shares.
Finally, this study will help future research to understand why firms in egypt and other emerging markets report their cybersecurity disclosures, as well as investigate what affect the scope of cybersecurity risks disclosure and how firms determine whether a particular information should be disclosed and how it should be disclosed. Another future research is to investigate whether the disclosed content is informative and valuable enough to help investors in decision making.
Funding : This research received no external funding.
Institutional Review Board Statement : Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest

References

1. Diane, J., Janvrin., Tawei, Wang. (2019). Implications of Cybersecurity on Accounting Information. Journal of Information Systems. https://doi:10.2308/ISYS-10715
2. Yang, L., Lau, L., & Gan, H. (2020). Investors' perceptions of the cybersecurity risk management reporting framework. International Journal of Accounting & Information Management, 28(1),167-183. https://doi.org/10.1108/IJAIM-02-2019-0022
3. Spanov, Y., & Alimzhanova, L. (2023). Identification of cybersecurity risks and threats to ensure the integrity of the financial sector. Journal of problem in computer science and information technologies, 1(1). https://doi.org/10.26577/JPCSIT.2023.v1.i1.06
4. Shaikh, F. A., & Siponen, M. (2023). Organizational Learning from Cybersecurity Performance: Effects on Cybersecurity Investment Decisions. Information Systems Frontiers, 1-12. https://doi. org/10.1007/s10796-023-10404-7
5. Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. Journal of Information Technology, 26, 60-77. https://doi.org/10. 1057/jit.2010.4
6. SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors https://doi.org/10.1016 /j.accinf.2018.06.003
7. Campbell, J. L., Chen, H., Dhaliwal, D. S., Lu, H. M., & Steele, L. B. (2014). The information content of mandatory risk factor disclosures in corporate filings. Review of Accounting Studies, 19, 396-455. https://link.springer.com/article/10.1007/s11142-0139258-3
8. Kwon, J., Ulmer, J. R., & Wang, T. (2013). The association between top management involvement and compensation and information security breaches. Journal of Information Systems, 27(1), 219-236. https://doi.org/10.2308/isys-50339
9. Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. SN Business & Economics, 3(5), 97. https://doi.org/10.1007/s43546-023-00477-6
10. Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Sohail, T. 2006. "The Impact of the Sarbanes Oxley Act on the Corporate Disclosures Concerning Information Security," Journal of Accounting and Public Policy (25:5), pp. 503-530. https://doi.org/10.1016/j.jaccpubpol.2006.07.005
11. Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. Information systems research, 24(2), 201-218. https://doi.org/10.1287/isre.1120.0437
12. Hilary, G., Segal, B., & Zhang, M. H. (2016). Cyber-risk disclosure: Who cares?. GeorgetownMcDonough School of Business Research Paper. https://papers.ssrn.com /sol3 /papers.cfm ?abstractid=2852519
13. Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. Journal of Accounting and Public Policy, 37(6), 508–526. https://doi.org/10.1016/j.jaccpubpol .2018.10.003

14. Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. International Journal of Accounting Information Systems, 38, 100468. https://doi.org/10.1016/j.accinf.2020.100468
15. Radu, C., & Smaili, N. (2022). Board gender diversity and corporate response to cyber risk: evidence from cybersecurity related disclosure. Journal of business ethics, 177(2), 351-374. https://doi.org/10.1007/s10551-020-04717-9
16. Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. Computers & Security, 58, 216–229. https://doi.org/10.1016/ j.cose.2015.12.006
17. Ilaria, Colivicchi., Riccardo, Vignaroli. (2019). Forecasting the Impact of Information Security Breaches on Stock Market Returns and VaR Backtest. Journal of Mathematical Finance, , 9, 402-454. https://hdl.handle.net/2158/1168410
18. Chai, S., Kim, M., & Rao, H. R. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. Decision Support Systems, 50(4), 651661.https://doi.org/10. 1016/j.dss.2010.08.017
19. 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
20. Daoud, M. M., & Serag, A. A. (2022). A proposed Framework for Studying the Impact of Cybersecurity on Accounting Information to Increase Trust in The Financial Reports in the Context of Industry 4.0: An Event, Impact and Response Approach. Journal of finance, tanta University, 42(1), 20-61. DOI: 10.21608/caf.2022.251730
21. Cheong, A., Yoon, K., Cho, S., & No, W. G. (2021). Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. Journal of information Systems, 35(2), 179-194. https://doi.org/10.2308/ISYS-2020-031
22. Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport informationon cyber-attacks? Evidence from capital markets. Review ofAccounting Studies, 23(3), 1177–1206. https://link.springer.com/article /10.1007/s11142-018-9452-4
23. Beatty, A., Cheng, L., & Zhang, H. (2019). Are risk factor disclosures still relevant? Evidence from market reactions to risk factor disclosures before and after the financial crisis. Contemporary Accounting Research, 36(2), 805–838. https://doi.org/10.1111/1911-3846.12444
24. Tosun, O. K. (2021). Cyber-attacks and stock market activity. International Review of Financial Analysis, 76, 101795. https://doi.org/10.1016/j.irfa.2021.101795
25. Campbell, J.L., Chen, H., Dhaliwal, D.S., Lu, H.-m., Steele, L.B., 2014. The information content of mandatory risk factor disclosures in corporate filings. Review of Accounting Studies.19(1), 396–455. https://link.springer.com/article/10.1007/s11142-013-9258-3
26. Hope, O. K., Hu, D., & Lu, H. (2016). The benefits of specific risk-factor disclosures. Review of Accounting Studies, 21(4), 1005–1045. https://link.springer.com/article/ 10.1007/s111 42 -016-9371-1
27. Securities and Exchange Commission (SEC), 2005. Release #33-8591: Securities Offering Reform (Section VII: Additional Exchange act Disclosure Provisions). Retrieved from https://www. sec.gov/spotlight/cybersecurity-roundtable.shtml
28. Nelson, K. K., & Pritchard, A. C. (2016). Carrot or stick? The shift from voluntary to mandatory disclosure of risk factors. Journal of Empirical Legal Studies, 13(2), 266–297. https://doi.org/10.1111/jels.12115
29. Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. International Journal of Accounting Information Systems, 30, 40–55. https://doi.org/10.1016/j.accinf.2018.06.003
30. Ali, S. E. A., & Lai, F. W. (2022, November). Cyber Security Breaches and the Long-Run Effect on Firms' Market Value: A Conceptual Framework. In International Conference on Artificial Intelligence for Smart Community: AISC 2020, 17–18 December, Universiti Teknologi Petronas, Malaysia (pp. 689-697). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-16-2183-3_66
31. Filzen, J. J., McBrayer, G. A., & Shannon, K. S. (2023). Risk factor disclosures: Do managers and markets speak the same language?. Accounting Horizons, 37(2), 67-83. https://doi.org/10.2308/HORIZONS-17-086
32. Chen, J., Henry, E., & Jiang, X. (2023). Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach. Journal of Business Ethics, 187(1), 199-224. https://link.springer.com/article/10.1007/s10551-022-05107-z
33. Calderon, T. G., & Gao, L. (2021). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. International Journal of Auditing, 25(1), 24-39. https://doi.org/10.1111/ijau.12209
34. Lenka, A., Goswami, M., Singh, H., & Baskaran, H. (2023). Cybersecurity Disclosure and Corporate Reputation: Rising Popularity of Cybersecurity in the Business World. In Effective Cybersecurity Operations for Enterprise-Wide Systems (pp. 169-183). IGI Global. DOI: 10.4018/978-1-6684-9018-1.ch008
35. Ramírez, M., Rodríguez Ariza, L., Gómez Miranda, M. E., & Vartika. (2022). The Disclosures of Information on Cybersecurity in Listed Companies in Latin America— Proposal for a Cybersecurity Disclosure Index. Sustainability, 14(3), 1390. https://doi.org/10.3390/su14031390

36. Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. Journal of Marketing, 82(2), 85–105. https://doi.org/10.1509/jm.16.0124
37. Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics, 139(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019
38. Bederna, Z., & Szádeczky, T. (2023). Managing the financial impact of cybersecurity incidents. Security and Defence Quarterly, 41.
39. Rosati, P., Gogolin, F., & Lynn, T. (2022). Cyber-security incidents and audit quality. European Accounting Review, 31(3), 701-728. https://doi.org/10.1080/09638180.2020.1856162
40. Musiał, N. (2019). Cyber risk in financial institutions: A Polish case. In Multiple Perspectives in Risk and Risk Management: ERRN 8th European Risk Conference 2018, Katowice, Poland, September 20-21 (pp. 301-313). Springer International Publishing. https://doi.org/10.1007/978-3-030-16045-6_16
41. Almasani, A. A., Azam, S. F., Ahmed, S., & Yusoff, S. K. B. M. (2019). The Mediation Effect of Audit Quality on the relationship between Auditor-Client Contracting Features and the Reliability of Financial Reports in Yemen. International Journal of Business Society, 3(10), 58-69. http://dx.doi.org/10.30566/ijo-bs/2019.109
42. Metlej, G., Zalzali, Y., & Farhat, M. (2021). The Impact of the Implementation of Financial Risks Management on the Disclosure Quality of Financial Reports. International Journal of Economics and Finance, 13(9), 61-83. https://doi.org/10.5539/ijef.v13n9p61
43. Frank, M. L., Grenier, J. H., Pyzoha, J. S., & Zielinski, N. B. (2023). Implications of EnhancedCybersecurity Risk Management Reporting and Independent Assurance. Current Issues in Auditing, 17(1), P11-P18. https://doi.org/10.2308/CIIA2022-018
44. Kassar, G. (2023,June). Exploring Cybersecurity Awareness and Resilience of SMEs amid the Sudden Shift to Remote Work during the Coronavirus Pandemic: A Pilot Study. In ARPHA Conference Abstracts (Vol. 6, p. e107358). Pensoft Publishers. https://doi.org/10.3897/aca.6.e107358
45. Smith, K. T., Smith, L. M., Burger, M., & Boyle, E. S. (2023). Cyber terrorism cases and stock market valuation effects. Information & Computer Security, 31(4), 385-403. https://doi.org/10.1108/ICS-09-2022-0147
46. Smith, K. T., Jones, A., Johnson, L., & Smith, L. M. (2019). Examination of cybercrime and its effects on corporate stock value. Journal of Information, Communication and Ethics in Society, 17(1), 42-60. https://doi.org/10.1108/JICES-02-2018-0010
47. Mohamed, A. (2020). The relationship between financial reporting quality and firm value of companies listed at the Nairobi securities exchange. http://erepository.uonbi.ac.ke/handle/11295/153926
48. Keman, Huang., Rebecca, Ye., Stuart, E., Madnick. (2019). Both Sides of the Coin: The Impact of Cyber Attacks on Business Value. Social Science Research Network. https://papers.ssrn.com/sol3/papers .cfm?abstract_id=3699756
49. Zhang, H., & Zhao, J. (2023). Stock market liberalization and financial reporting quality. China Journal of Accounting Research, 16(4), 100328. https://doi.org/10.1016/j.cjar.2023.100328
50. Ali, J. S. (2018). Effect of financial reporting quality on the market price per share of firms listed in the Nairobi Securities Exchange. http://41.89.49.13:8080/xmlui/handle/123456789/1405
51. Baig, A., Blau, B. M., & Griffith, T. G. (2021). Firm opacity and the clustering of stock prices: the case of financial intermediaries. Journal of Financial Services Research, 60(2), 187-206. https://doi.org/10.1007/s10693-020-00341-w