The effect of CSR on the interrelationship among cyber risk, supply chain, and small and medium-sized enterprises performance

(An Applied Study)

تأثير المسؤولية الاجتماعية للشركات على العلاقة المتبادلة بين المخاطر السيبرانية وسلسلة التوريد وأداء الشركات الصغيرة والمتوسطة الحجم

(دراسة تطبيقية)

Dr. Mohamed Hassan Abd-Elmageed

Assistant Professor of Accounting Faculty of Business – Ain Shams University

Dr.mohamedabdelmageed@bus.asu.edu.eg

المستخلص:

لقد استحوذت الإحتمالات المتزايدة للإنتهاكات السيبرانية كمصدر للمخاطر على إهتمام الشركات والباحثين للتحقيق في آثارها وطرق الحد منها. ولقد برزت المسؤولية الإجتماعية للشركات كوسيلة للتأثير على الإنطباعات الشخصية للمتلقي التي يمكن أن تخفف من عواقب المخاطر السيبرانية. وتتمتع الشركات الصغيرة والمتوسطة الحجم عادة بسياق فريد للتدقيق في هذا الموضوع خاصة مع حساسية العائد على الإستثمار وقيود الموارد. ويهدف البحث الي تحليل تأثير المسؤولية الاجتماعية للشركات على الأمن السيبراني من منظور أصحاب المصلحة، وتحديد ردود أفعال الموردين تجاه الأمن السيبراني، واستكشاف الآثار المترتبة على بيئة الشركات الصغيرة والمتوسطة الحجم في ضوء المخاطر السيبرانية وردود أفعال الموردين والعلاقات مع العملاء

وقد اثبتت الدراسة أن هناك علاقة طردية بين المسئولية الاجتماعية للشركات وتصورات الأمن السيبراني، كما ان هناك علاقة طردية بين مخاطر الأمن السيبراني وتوازن العلاقة بين المورد والعميل، وأن هناك علاقة عكسية بين مخاطر الأمن السيبراني والعائد على الاستثمار، وأن المسئولية الاجتماعية للشركات و/ أو مخاطر الأمن السيبراني و/ أو الترابط في سلسلة التوريد لها تأثير على أداء الشركات الصغيرة والمتوسطة الحجم.

الكلـمات المفتـاحية:

المسؤولية الإجتماعية للشركات، الأمن السيبراني، المخاطر السيبرانية، سلسلة التوريد، المؤسسات الصغيرة والمتوسطة الحجم، إدارة الانطباع، نظرية المعالجة المزدوجة.

Abstract:

Recent increasing potential of cyber breaches as a risk source has grasped the attention of firms and scholars to investigate their implications and ways to mitigate. Corporate social responsibility (CSR) has emerged as a means of impression management that possibly can alleviate cyber risk consequences. Small and medium enterprises (SMEs) have a unique context to scrutinize this theme especially with their return on investment sensitivity and resource constraints. The research aims to analyze the impact of corporate social responsibility on cybersecurity from the perspective of stakeholders, identify suppliers' reactions to cybersecurity, and explore the implications for small and medium-sized enterprises considering cybersecurity risks, suppliers' responses, and customer relationships.

The study has demonstrated that there is a direct relationship between corporate social responsibility and perceptions of cybersecurity, as well as a direct relationship between cybersecurity risks and the balance of the supplier-customer relationship. Furthermore, there is an inverse relationship between cybersecurity risks and return on investment, and that corporate social responsibility and/or cybersecurity risks and/or supply chain interconnectivity have an impact on the performance of small and medium-sized enterprises.

Keywords: Corporate social responsibility (CSR), cyber security, cyber risk, supply chain, small and medium enterprises (SME), impression management, dual processing theory.

INTRODUCTION

Recently, the waves of digital transformation have pushed small and medium-sized enterprises (SMEs) to embrace and equip their business models with ever-evolving technologies (Jafari-Sadeghi et al., 2021). Whether online shopping (Tarhini et al., 2018) or running supply chains of firms (Dallasega et al., 2018), technological advancement has resulted in stimulating business opportunities (Soomro et al., 2016), and it has also escorted to novel challenges that amended organizational designs, the capability to manage data, and a new source of risks (Calabrese et al., 2019; Jafari-Sadeghi, 2021; Shah et al., 2019). In fact, emerging obstacles like information security and cyber risks have led to widespread financial and nonfinancial losses (Arcuri et al., 2017). Relatedly, SMEs are supposed to face the same levels of cybersecurity issues as their larger counterparts, however, limited resources and capabilities made them weak against cyber-risks (Baggott & Santos, 2020; Benz & Chatterjee, 2020). Cyber risk management and preparation are currently regarded as crucial competencies for not only survival but also the growth of small firms (Chatterjee, 2019; Hoppe et al., 2021).

Due to the popularity and severity of cybersecurity incidents rising, investors are actively searching for information about how companies are managing cybersecurity risk (EY 2020; Center for Audit Quality (CAQ) 2020).

However, the real impacts of cyber breaches are much more noteworthy, difficult to quantify, and hidden from public view (Deloitte 2016). One of these hidden costs is the impact of cyber breaches on supply chain partners. Recent surveys specify that cyber breaches are the most impactful event to supply chain stability, and cybersecurity threat is listed as the number one threat to global supply chain partners (Rajagopal 2019; DHL 2020). Even though the National Institute of Standards and Technology has focused on driving awareness of supply chain cyberattacks since 2008, the number of attacks increased significantly each year (Symantec 2019). Present literature using surveys and experiments suggests cyber breaches damage firms' stakeholders, such as customers and suppliers (Hovav and Gray 2014; Veltsos 2012; Janakiraman, Lim, and Rishika 2018). However, there is little empirical evidence on how cyber breaches affect supply chain partners. Motivated by the real-world incidents and industry experts' consensus, this paper investigates whether customers' cyber breaches negatively influence suppliers' innovative investments.

It is imperative for companies to implement damage control and remedial strategies to mitigate investors' negative reactions to the occurrence of cybersecurity breaches (e.g., impaired investor confidence and consequently reduced investment). Currently, there is little accounting research examining the use of remedial strategies for cybersecurity breaches (Walton, Wheeler, Zhang, and Zhao 2021; Kelton and Pennington 2020). In addition, the limited research on remedial strategies (e.g., Choi, Kim, and Jiang 2016; Goode, Hoehle, Venkatesh, and Brown 2017) tends to focus on passive responses that are deployed after negative events have occurred. Although important, these reactive responses are generally less effective as they tend to be perceived as an effort to restore the company's image rather than actions from its real interests (Rim and Ferguson 2020). It is crucial to investigate whether and how proactive, insurance- like remedial strategies could help organizations temper investors' negative reactions.

When implementing remedial strategies, firms can focus on strategies that directly target their IT management. For example, a variety of IT governance frameworks (e.g., Objectives for Information and related Technology (COBIT) and International Organization for Standardization (ISO) 27001) provide a structure for organizations to ensure that their IT assets are well protected, and IT investment supports business objectives.

Alternatively, firms can implement indirect strategies that promote stakeholders' overall impression/perception of the firm and thus can serve as a buffer when negative events, including cybersecurity breaches, occur. Among various practices, corporate social responsibility (CSR) has been regarded as central in promoting firms' overall image (Kim, Yin, and Lee 2020; Perez and del Bosque 2015). Binkley (2021) proposes that CSR activities are associated with improvements in the quality and reliability of information used for enterprise risk management (Casey and Grenier 2015) and therefore should be a component of a holistic approach to IT risk management (Binkley 2021).

Research objectives:

1- Identify how CSR can affect cybersecurity perceptions in the eyes of stakeholders.
2- Identify supplier reactions to cybersecurity efforts.
3- Explore the SME environment implications for cyber risk and supplier – customer relations.

LITERATURE AND HYPOTHESES DEVELOPMENT

1) The relationship between Cybersecurity & CSR:

Outstanding CSR performing can generate moral capital for a firm by indicating a willingness to act humanitarian (Godfrey et al. 2009). This moral capital can result in insurance-like protection to the company and mitigate negative consequences in the occurrence of harmful events (Godfrey et al. 2009; Liu et al. 2020). Many studies have specified substantiation in support of the insurance-like effects of CSR on cases of unrelated adverse events. For instance, Klein and Dawar (2004) find that superior CSR cuts the adverse impact of a product-harm crisis on consumers' brand evaluations and purchase intention. Godfrey et al. (2009) affirm that participation in CSR activities lessens stakeholders' adverse judgments and sanctions through legal and regulatory actions in opposition to firms.

CSR can lessen investors' adverse reactions after cybersecurity breaches. Specifically, based on dual-processing theories (e.g., Evans 2006, 2008; Kahneman 2011; Hamilton and Winchel 2019), it is believed that CSR can potentially impact investors' judgment by two processes. Dual-processing theories suggest that two distinctive systems exist in the human brain to process information. Process one is automatic, quick, effortless, heuristics-based, and dependent on intuition (Farrell, Goh, and White 2014; Gette, Kryjevskaia, Stetzer, and Heron 2018). Process two on the other hand, is regarded as diagnostic, deliberated, slow, reflective, rule-based, and effortful. In the view of default-interventionist, process one is thought to be the default system (Pennycook, Fugelsang, and Koehler 2015) which can be activated automatically. However, process two monitors the processing of process one, deciding on whether to override the judgment of process one. When process two does intervene, it results in deliberative cognitive processing to decide whether to override the judgment of process one. If the judgment is similar, the judgment of process one will be strengthened. If the judgment is divergent, the judgment of process one will be replaced.

First CSR can affect investor judgment through process one by inducing affective reactions. As mentioned, the processing of process one is heuristics-based and dependent on affect and intuition. One such heuristic is affect-as-information (Farrell et al. 2014). Affect-as-information heuristics (Schwarz and Clore 1983, 2003) imply that individuals can use their affect or feelings as heuristically relevant information to make consequent judgments (Kadous 2001; Elliott, Jackson, Peecher, and White 2014). Specifically, affective feelings will operate as important reference criteria and impact both the process and outcome of judgment formation (Seo, Barrett, and Bartunek 2004).

CSR can operate as a quality seal representing organizations' compliance with best practices and high-level standards. Consequently, compared to no corporate social irresponsibility

(CSI), corporate social responsibility (CSR) is likely to induce more positive affect in investors and influence investors' subsequent attitudes and judgments. In other words, in the occurrence of cybersecurity breaches, investors should have less negative affect toward the company if the company has been attached to CSR than a company recognized as socially indifferent or negligent.

Second, being a CSR compliant may also affect investors through process two by engaging in systematic and deliberate cognitive processing, thus strengthening the judgment of process one. Attribution Theory (Weiner 1979, 1985, 1986) suggests that people often try to understand why certain events occur, especially when the outcome is negative or unexpected (Schatt 2011). Specifically, people will attempt to understand the cause of the event in terms of locus, controllability, and stability (Graham 1991). The pointed pivot outlines the location of the cause as internal or external to the individual/entity. Among different causes, ability and effort are considered to be the most dominant internal causes as they indicate the characteristics of the entity (Graham 1991). People are inclined to attribute failure to a lack of ability and/or effort while success is more attributed to high ability and effort.

According to Attribution Theory, when a cybersecurity breach occurs, investors will try to understand the cause of the event. In particular, investors will assess the firm's ability and effort to be responsible to their society. Those firms will be perceived to be more capable of and diligent in protecting information security. Consequently, investors should be less likely to attribute the cybersecurity breach event to the firm and more likely to attribute the event to external/situational factors (after all, data breaches could even occur to the greatest companies). This attribution will in turn influence investors' trust in companies' internal control system. Investor trust plays a critical role in managing negative events (Elliott, Hodge, and Sedor, 2012). Elliott et al. (2012) show that attribution alters investor trust and ultimately affects their investment decisions.

Corporate social irresponsibility (CSI) influences employees and external hackers in a way that affects intentional data breaches. In terms of employees, it is proposed that CSI triggers employees' anomalous security behaviors since it breaches their legitimate job demands. First, employees have personal interest-based instrumental demands, which include job security, fair financial compensation, and opportunities for training and career development (Du et al., 2015). Second, employees have ideology-based demands (Du et al., 2015). These demands are related to how companies deal with the broader society and the opportunities they provide for employees to participate in pro-social activities.

CSI violates both the instrumental and ideological demands of employees. As a severe crisis, CSI can weaken a company's financial performance and terrorize its survival (Liang et al., 2016). To confront such a crisis, firms often decrease employee benefits and even cut the workforce, putting employees' instrumental benefits in danger. Further, CSI tends to be at odds with the morals and values that employees hold (Jang et al., 2022) leading to the breach of ideological demands.

The legitimacy perspective claims that employees cultivate negative feelings, attitudes, and workplace behaviors as repercussions when their legitimate job demands are broken (Wang et al., 2021). Breaching instrumental demands pushes employees to experience job dissatisfaction and the desire to quit (Sirota et al., 2005). Severe shame resulting from CSI can reduce employees' identification with and commitment to their companies (Cole et al., 2010, Lee and Yoon, 2018, and Onkila, 2015).

Other studies have indicated that CSI causes adverse employee behaviors, including counterproductive behaviors (Cohen-Charash and Spector, 2001) and divergent workplace behaviors (e.g., sabotage).

Negative employee emotions and perceptions are argued to be salient drivers of data breaches (Burns, 2023, Willison and Warkentin, 2013).

Studies have found that negative workplace emotions, such as disharmony, induce internal hacking activities (Maasberg, 2020, and Liang, 2016).

Research has also documented that employees' security behaviors depend largely on how they cognitively and emotionally feel about their organizations. Employees who feel low commitment to their employers are less likely to exert cognitive efforts to comply with information security policies (Hsu, 2015). Furthermore, there are claims that moral incongruence can be an outstanding source of motivation for employee hacking (Son, 2011).

External hackers may also extend hacking motives due to CSI. There may be a moral compass directing hackers to amend perceived wrongs. As CSI confirms a firm's self-serving actions, that often come at the cost of stakeholder value or greater social good, it is inclined to be at odds with hackers' moral beliefs and cause their attacks (D'Arcy, 2020). From an opportunity standpoint, CSI may offer hackers with strategic opportunities for attacks. CSI firms usually divert huge resources and attention toward crisis management, fading cybersecurity efforts. Moreover, the outpouring of internal and external threats may overwhelm security professionals, making it demand to punctually identify, deter, and trace attacks (Mitra and Ransbotham, 2015). From a cost perspective, targeting socially irresponsible companies is attached to less moral costs (Brauer and Tittle, 2017) as hackers can undoubtedly justify their actions (Young, 2007).

In sum, the researcher proposes the following hypothesis:

$\boldsymbol{H_{01}}$: There is no direct relationship between corporate social responsibility and cybersecurity perceptions.

2) The relationship between Cybersecurity & supply chain:

Resource dependence theory (RDT) indicates how organizations manage resources to alleviate external uncertainties and interdependence (Pfeffer and Salancik 1978). The premise of RDT is the importance of resources as firms depend on resources to function. Resources, to a great deal, are part a firm's environment, and RDT identifies that organizations are rooted in networks of interdependencies and social relationships and therefore are subject to contingencies in the external environment (Pfeffer and Salancik 1978; Hillman, Withers, and Collins 2009). Managers act to secure resources by alleviating environmental uncertainty and dependence (Hillman, Withers, and Collins 2009). To alleviate dependencies on external resources, firms align their internal elements to deal with internal resource allocations (Pfeffer 1987). RDT predicts that in a business-dependent relationship, each business partner tends to amend their level of ongoing investments in this relationship to alleviate interdependencies when facing external challenges. A firm can be effective if it recognizes the pressure from its environment and adjusts itself to these contingencies. There are two resource dependence conditions. One is the uncertainty of resources supply, and the other is the need for more or better resources (Cheng and Bozeman 1993).

Due to resource dependency and limitations, firms are sensitive to external factors and situations that may cause supply chain disruption and affect their interorganizational relationships (Trkman and McCormack 2009). Firms react to these externalities by adjusting their behaviors and operations to preserve resources and reduce uncertainty and dependence (Chatterjee and Ravichandran 2013; Hillman et al. 2009). Various types of risk factors may cause supply chain disruption, like natural disasters or human-related issues (Trkman and McCormack 2009). Therefore, it is vital for suppliers to detect the resources that may be impacted by market turbulence and make strategic plans to protect firm resources against potential disruptions to the supply chain.

Customer cyber breaches may impact both customer and supplier's profitability and hence reduce the deal of resources available to allocate to innovation (He et al. 2020; Lattanzio and Ma 2021; Hsu et al. 2021; Garg 2020). Cyber breaches could impact a customer's financial stability, resulting in financial risks for the supplier. Cyber breaches are also linked to high operational costs for breached firms, such as system recovery, legal fees, product liability, and potential litigation and hence directly impact a firm's profitability and cash flow (Ponemon Institute 2020). Under these situations, a breached customer may become sensitive to prices and try to increase profit margins to offset increased costs. Therefore, the customer may be more likely to bargain over costs or defer payment terms, reducing supplier margins. Further, suppliers increase their cash holdings following a customer cyber breach (Garg 2020). Reduced supplier profitability or increased cash holdings leave the suppliers with fewer resources to allocate to innovative investments (Krolikowski and Yuan 2017).

Customer cyber breaches can discourage information sharing and hinder collaborative R&D between supply chain partners. Customer cyber breaches may hinder information exchange as the consequences of cyber breaches at the customer may not be observable by the supplier, thus elevating information asymmetry between the two parties.

Firms suffering from cyber breaches are also more likely to engage in opportunistic behaviors (Xu et al. 2019), limiting effective and transparent information sharing with their supply chain partners. This information barrier because of major customer's cyber breaches creates hurdles for the cooperative and interactive innovation process.

Lastly, cyber breaches jeopardize trade secrets and other proprietary information, which provides future economic value and leads to patent and product or technology innovation (Glaeser

2018; Basuchoudhary and Searle 2019). Ettredge, Guo, and Li (2018) claim that firms with trade secrets are more likely to be targeted by hackers. A Deloitte (2016) survey exposes that the loss of intellectual property because of cyber breaches enforces high intangible costs on the breached firms and may lead to loss of competitive advantages. Facing high cyber risks, a firm may proactively cut innovation and adjust its innovation policies to protect its intangible and intellectual property (He et al. 2020; Lattanzio and Ma 2021). Moreover, information leakage from one supply chain partner may create a high cyber risk and information risk to the rest of the trading partners as the supply chain network forms an integrated information sharing system (Symantec 2019). To address the accelerated information risks surrounding its own innovation due to customer cyber breaches, a supplier is likely to adjust its own level of innovation to protect its proprietary information that leads to innovation.

When a major customer incurs a cyber breach, its suppliers respond to such an event by assessing their own potential risks and making corresponding strategic changes to preserve resources to shield themselves from uncertainties. Customer cyber breaches not only affect contract reliability but also impose a threat to information leakage and future breaches of the suppliers. When the customer’s system stability and information quality are at risk, the supplier might temporarily quit or postpone transactions with the customer to protect their proprietary information, causing customer-supplier relationship disruption.

Therefore, the second hypothesis can be stated as follows:

$\boldsymbol{H_{02}}$: There is no direct relationship between cybersecurity risks and supplier-customer relationship disruption.

3) The relationship between Cybersecurity & SME:

Consistent with a survey of nonprofessional investors, 84 percent of the respondents report that cybersecurity threats influence their investment decisions (Center for Audit Quality 2017).

Sangani and Vijayakumar (2012) stress that large firms have the technological expertise to defense their company’s information assets and the resources to shield against cyber threats by capital investment in security tools and employee training, nevertheless when it comes to SMEs, their resource constraints can form a barrier to address cyber threats and can expose them to financial and reputational damages.

Although extensive studies have examined the impact of information and communication technology usage from an SME perspective (Mustafa & Yaakub, 2018), studies about their cyber risks and assessment are still emerging. A study by Eilts and Levy (2018) remarked the cybersecurity awareness of SMEs while Lewis et al. (2014) addressed cybersecurity related to SME supply chains. Decision making in small-scale IT users was studied by Osborn and Simpson (2017), with cyber- security practices of SMEs in developing countries explored by Kabanda et al. (2018).

Examining the literature, one can observe that when it comes to cyber risks, there are very few studies that have delved into either assessment or risk evaluation in an SME context.

From the perspective of SMEs, there are knowledge gaps regarding how risk is prioritized, how risks are assessed, and tactics for mitigation. When one takes into account, the differences in firm characteristics and entrepreneurial risk profiles of individuals associated with SMEs (Ratten, 2019), there is a drought of research examining how cyber risk management is undertaken in SMEs. The study of cyber risk management practice in SMEs is vital due to the role played by them in the socioeconomic development of a nation.

As opposed to the contribution of SMEs, a recent study also notes that four in ten SMEs have experienced cyberattacks in the 12 months (Rae & Patel, 2019) and only 14% of microenterprises are keenly involved in Information and Communication Technology (ICT) risk assessments (Office for National Statistics, 2019). Given the contribution of SMEs and the deficiency of risk assessment techniques in their context, there is a need to address this. The existing approaches either based on technical risk analyses or risk-based decision analysis have not specifically targeted SMEs nor have attempted to develop a framework for assessment and management.

Perols (2024) uncover evidence that investors are sensitive to cyber risks and distinguish more comprehensive cybersecurity examinations to provide higher assurance service quality, resulting in an increased willingness to invest . Dual processing theories as mentioned distinguish between simple heuristic processing (i.e., peripheral route or process one) and effortful systematic processing (i.e., central route or process two) (Chaiken 1980; Petty and Cacioppo 1986; Chaiken and Maheswaran 1994; Kahneman 2003). In heuristic processing, individuals depend on easily available cues to alleviate information processing demands when evaluating new information (Chaiken 1980; Petty and Cacioppo 1986; Chaiken and Maheswaran 1994; Kahneman 2003). In systematic processing, individuals have the inspiration and skill to use more effortful processing and are more likely to aggressively address the content of the information being processed (Chaiken and Maheswaran 1994; Kahneman 2003). Contextual variables can affect individuals' enthusiasm to engage in effortful systematic processing ahead of simple heuristic processing (Chaiken 1980; Petty and Cacioppo 1986; Chaiken and Maheswaran 1994; Kahneman 2003).

Regarding dual processing theories application to the cybersecurity disclosure setting, during the nonexistence of a cybersecurity incident, nonprofessional investors are more likely to experience simple heuristic processing and depend primarily on straightforwardly accessible cues, leading to taking no notice of to the type of external cybersecurity assurance service and being assured of the investing decisions. On the other hand, a contextual variable, such as a cybersecurity incident, has the potential to motivate investors to engage in effortful systematic processing, resulting in enhanced attention to the information about the cyber-risk and being reluctant to invest.

Cybersecurity breaches levy extremely high costs on breached firms. Ponemon Institute (2020) assesses the average cost of a data breach is $3.86 million per incident. cyber breaches threaten a firm’s intellectual property, harmfully affect firms’ market value, interrupt operations, intrude business practices, harm firms’ reputation, and contribute to financial distress (Deloitte 2016; Basel Committee on Banking Supervision 2014; Mossburg, Gelinne and Calzada 2016; Hovav and Gray 2014; Gwebu, Wang, and Xie 2014; Confente, Siciliano, Gaudenzi, and Eickhoff 2019).

Suffering high financial penalties, breached firms react to cyber breaches by amending their strategic decisions on cash holdings (Garg 2020), finance policies (Boasiako and Keefe 2021), reporting behaviors (Xu, Guo, Haislip, and Pinsker 2019), and investment activities (He, Frost, and Pinsker 2020) to alleviate cyber breaches’ negative impacts.

Therefore, the third hypothesis will be:

$\boldsymbol{H_{03}}$: There is no negative relationship between cyber-risk and return on investment.

Considering all the discussed interrelationships, the fourth hypothesis will be:

$\boldsymbol{H_{04}}$: Corporate social responsibility and / or Cybersecurity Risks, and /or Supply Chain interdependencies have no impact on SMEs Performance.

Population and sample size:

Data were collected cross sectional data from 37 companies listed under EGX_100, thus the final sample size is 37 companies each one has an annual time series of 1 year which is 2023. So, the total final number of the applied study sample is 37 observations.

Descriptive Analysis:

The researcher will analyze the study variables in order to determine the variables measures of central tendency which are: weighted average mean, minimum and maximum values, also will presents measures of dispersion which are presented in standard deviation and coefficient of variation in order to determine the percentage of variability for each variable, as presented in table (1).

Table (1): Variables descriptive analysis

Variable	n	Min.	Max.	Mean	Standard Deviation	Coefficient of Variation
Corporate Social Reasonability	37	1.00	5.00	3.75	0.92	0.24
Cybersecurity Perception	37	2.24	5.00	3.79	0.80	0.21
Cybersecurity Risks	37	2.60	5.00	4.10	0.60	0.15
Inventory Turnover	37	0.03	1.30	0.48	0.38	0.78
Return on Investments	37	0.06	0.64	0.24	0.15	0.62

Source: prepared by the researcher from E-views software output.

From table (1) it is noted that:

1- All variables have 37 observations which mean that there is no missing data.

2- Corporate Social Reasonability has a minimum value of 1.00 and maximum value of 5.00 with a weighted average mean of 3.75, and its standard deviation is 0.92 and coefficient of variation of 24% which indicates a low level of dispersion of values around their weighted average mean.

3- Cybersecurity Perception has a minimum value of 2.24 and maximum value of 5.00 with a weighted average mean of 3.79, and its standard deviation is 0.80 and coefficient of variation of 21% which indicates a low level of dispersion of values around their weighted average mean.

4- Cybersecurity Risks has a minimum value of 2.60 and maximum value of 5.00 with a weighted average mean of 4.10, and its standard deviation is 0.60 and coefficient of variation of 15% which indicates a low level of dispersion of values around their weighted average mean.

5- Inventory Turnover has a minimum value of 0.03 and maximum value of 1.30 with an arithmetic mean of 0.48, and its standard deviation is 0.38 and coefficient of variation of 78% which indicates a moderate level of dispersion of values around their arithmetic mean.

6- Return on Investments has a minimum value of 0.06 and maximum value of 0.64 with an arithmetic mean of 0.24, and its standard deviation is 0.15 and coefficient of variation of 62% which indicates a moderate level of dispersion of values around their arithmetic mean.

7- The dispersion values range from low to moderate levels of dispersion according to coefficient of variation measurement due to the sample diversification, as the sample consists of different companies from different sectors with different natures under$\boldsymbol{EGX_{90}}$, in order to make the sample present the whole index and not being biased.

Test of normality:

The study applied Shapiro-Wilk test to determine whether the main variables of study follow the normal distribution or not. Shapiro-Wilk test is a Chi-squared test of normality which its null hypothesis states that variables are not normally distributed if the test *p-value* is less than or equal 0.05, while its alternative hypothesis states that variables are normally distributed if the test *p-value* is more than 0.05, and the test for variables presented in the following table (2).

Table (2): Shapiro-Wilk test of normality

Variable	Statistic	*df*	*P-value*
Corporate Social Reasonability	0.933	37	*0.000*
Cybersecurity Perception	0.941	37	*0.000*
Cybersecurity Risks	0.943	37	*0.000*
Inventory Turnover	0.904	37	*0.000*
Return on Investments	0.924	37	*0.000*

Source: prepared by the researcher from E-views software output.

From table (2) it is concluded that all the independent, the moderator variable, and dependent variables are not normally distributed as their *p-value* of Chi-square statistic is less than 0.05, so the alternative hypothesis will be accepted that variables are not follow the normal distribution.

Correlation Matrix:

After applying test of normality for the independent sub-variables, moderator and the dependent sub-variables of study, it is found that the study variables don't follow the normal distribution, So Spearman correlation coefficient will be the most appropriate coefficient for determining the relation strength and direction between each two variables, then the correlation coefficient is tested by a t-test which its null hypothesis states that correlation does not exist if the test *p-value* is greater than 0.05.

The following table (3) presents the relations between the applied study variables.

Table (3): Spearman correlation matrix

Variable	Corporate Social Reasonability	Cybersecurity Perception	Cybersecurity Risks	Inventory Turnover	Return on Investments
Corporate Social Reasonability	**1.00**				
P-value	-				
Cybersecurity Perception	0.671**	**1.00**			
P-value	*0.000*	-			
Cybersecurity Risks	-0.267**	-0.331*	**1.00**		
P-value	*0.000*	*0.045*	-		
Inventory Turnover	0.467**	0.674**	-0.125**	**1.00**	
P-value	*0.004*	*0.000*	*0.000*	-	
Return on Investments	-0.184**	0.101*	-0.167**	0.209**	**1.00**
P-value	*0.000*	*0.046*	*0.000*	*0.000*	-

Source: prepared by the researcher from E-views software output.

*: refers to significance level of 5%.

**: refers to significance level of 1%.

From Matrix (3) it is noted that:

1- There is a significant, direct, and moderate relation between Corporate Social Reasonability and Cybersecurity Perception with correlation coefficient value of 0.671 and *P-value* 0.000.
2- There is a significant, inverse, and weak relation between Corporate Social Reasonability and Cybersecurity Risks with correlation coefficient value of -0.267 and *P-value* 0.000.
3- There is a significant, direct, and weak relation between Corporate Social Reasonability and Inventory Turnover with correlation coefficient value of 0.467 and *P-value* 0.004.
4- There is a significant, inverse, and weak relation between Corporate Social Reasonability and Return on Investments with correlation coefficient value of -0.184 and *P-value* 0.000.
5- There is a significant, direct, and moderate relation between Cybersecurity Perception and Inventory Turnover with correlation coefficient value of 0.674 and *P-value* 0.000.
6- There is a significant, direct, and weak relation between Cybersecurity Perception and Return on Investments with correlation coefficient value of 0.101 and *P-value* 0.046.
7- There is a significant, inverse, and weak relation between Cybersecurity Risks and Inventory Turnover with correlation coefficient value of -0.125 and *P-value* 0.000.
8- There is a significant, inverse, and weak relation between Cybersecurity Risks and Return on Investments with correlation coefficient value of -0.167 and *P-value* 0.000.

Testing the research Hypotheses:

Testing the First Hypothesis:

For testing the first hypothesis which is there is no direct relationship between corporate social reasonability and cybersecurity perceptions, the following table (4) presents simple linear regression model depending on a cross-section data which consists of 37 companies for year 2023 to test this hypothesis.

Table (4): The simple linear cross section regression model of the first hypothesis H_1

Model	*Simple Cross-section*	**Dependent variable**		Cybersecurity Perceptions	**VIF Test**
Independent variables	***Coefficient***	***t-ratio***	***p-value***	**Significance**	
Constant	1.37297	3.540	0.0012	**Significant**	
Corporate Social Reasonability	0.644949	6.409	<0.0001	**Significant**	1.000
F-test	41.07452	***p-value***		<0.0001	
Ramsey Reset test	3.02331	***p-value***		0.0622808	
Heterosckadicity test	1.78113	***p-value***		0.410423	
Adjusted R-squared			12.6780%		

Source: Prepared by the researcher depending on E-views software output.

From table (4) it is noted that:

1- The overall simple linear regression model depending on a cross-section data is significant as the overall F-test for significance has a value of 41.07452 and *p-value* <0.0001 which is less than 0.05, with adjusted R-squared value of 12.6780% which means that the independent variable explains 12.6780% of the change in the Cybersecurity perceptions.

2- Corporate Social Reasonability has direct and significant impact on cybersecurity Perceptions.

3- Corporate Social Reasonability coefficient shows direct and significant relation cybersecurity Perceptions.

4- There is no problem of multi-collinearity between the independent variables as the VIF test showed the result of one for the independent variable.

5- The Ramsey reset test has a *p-value* of 0.0622808 which is greater than 0.05, which means that the independent variables in the models are sufficient.

6- The Heterosckadicity test has *p-values* of 0.410423, which means that the residuals have a constant variance on long run and the model does not suffer from Heterosckadicity problem.

7- The overall equation for forecasting the cybersecurity Perceptions is:

$$\widehat{\text{cybersecurity Perceptions}}_i = 1.37297 + 0.644949\ \text{CSR}_i$$

Therefore, the researcher will reject the null hypothesis and accept the alternative hypothesis of the first hypothesis which means that there is a direct relationship between corporate social reasonability and cybersecurity perceptions.

Testing the second Hypothesis:

For testing the second hypothesis which is there is no direct relationship between cybersecurity risk and supplier-customer relationship disruption (presented in inventory turnover), the following table (5) presents simple linear regression model depending on a cross-section data which consists of 37 companies for year 2023 to test this hypothesis.

Table (5): The simple linear cross section regression model of the second hypothesis H_2

Model	*Simple Cross-section*	**Dependent variable**		Inventory Turnover	**VIF Test**
Independent variables	***Coefficient***	***t-ratio***	***p-value***	**Significance**	
Constant	−0.705229	−3.080	0.0040	**Significant**	
Cybersecurity Risk	0.314070	5.311	<0.0001	**Significant**	1.000
F-test	28.20433	***p-value***		<0.0001	
Ramsey Reset test	0.427942	***p-value***		0.655415	
Heterosckadicity test	8.028183	***p-value***		0.18059	
Adjusted R-squared			13.0419%		

Source: Prepared by the researcher depending on E-views software output.

From table (5) it is noted that:

1- The overall simple linear regression model depending on a cross-section data is significant as the overall F-test for significance has a value of 28.20433 and *p-value* <0.0001 which is less than 0.05, with adjusted R-squared value of 13.0419% which means that the independent variable explains of 13.0419% the change in the Inventory turnover.

2- Cybersecurity Risk has a direct and significant impact on inventory turnover.

3- Cybersecurity Risk coefficient shows direct and significant relation inventory turnover.

4- There is no problem of multi-collinearity between the independent variables as the VIF test showed the result of one for the independent variable.

5- Ramsey reset test has a *p-value* of 0.655415 which is greater than 0.05, which means that the independent variables in the models are sufficient.

6- Heterosckadicity test has *p-values* of 0.18059, which means that the residuals have a constant variance on long run and the model does not suffer from Heterosckadicity problem.

7- The overall equation for forecasting the Inventory Turnover is:

$$\widehat{\text{Inventory Turnover}_\text{i}} = -0.705229 + 0.314070\ \text{Cybersecurity Risk}_\text{i}$$

Therefore, the researcher will reject the null hypothesis and accept the alternative hypothesis of the second hypothesis which means that there is a direct relationship between cybersecurity risk and supplier-customer relationship disruption.

Testing the third Hypothesis:

For testing the third hypothesis which is there is no negative relationship between cybersecurity risk and return on investment, the following table (6) presents simple linear regression model depending on a cross-section data which consists of 37 companies for year 2023 to test this hypothesis.

Table (6): The simple linear cross section regression model of the third hypothesis H_3

Model	*Simple Cross-section*	**Dependent variable**		Return on Investment	**VIF Test**
Independent variables	***Coefficient***	***t-ratio***	***p-value***	**Significance**	
Constant	0.439191	2.561	0.0152	**Significant**	
Cybersecurity Risk	−0.0483444	−4.173	<0.0001	**Significant**	1.000
F-test	4.351594	***p-value***		0.003338	
Ramsey Reset test	0.254224	***p-value***		0.777119	
Heterosckadicity test	1.91921	***p-value***		0.383044	
Adjusted R-squared			11.0235%		

Source: Prepared by the researcher depending on E-views software output.

From table (6) it is noted that:

1- The overall random panel model is significant as the overall F-test for significance has a value of 4.351594 and *p-value* 0.003338 which is less than 0.05, with adjusted R-squared value of 11.0235% which means that the independent variable explains 11.0235% of the change in the Return on Investment.

2- Cybersecurity Risk has inverse and significant impact on Return on Investment.

3- Cybersecurity Risk coefficient shows inverse and significant relation Return on Investment.

4- There is no problem of multi-collinearity between the independent variables as the VIF test showed the result of one for the independent variable.

5- Ramsey reset test has a *p-value* of 0.777119 which is greater than 0.05, which means that the independent variables in the models are sufficient.

6- The Heterosckadicity test has *p-values* of 0.383044, which means that the residuals have a constant variance on long run and the model does not suffer from Heterosckadicity problem.

7- The overall equation for forecasting the Return on Investment is:

$$\text{Return on }\widehat{\text{Investment}}_{i} = 0.439191 - 0.0483444\ \text{Cybersecurity Risk}_{i}$$

Therefore, the researcher will reject the null hypothesis and accept the alternative hypothesis of the third hypothesis which means that there is an inverse relationship between cybersecurity risk and Return on Investment.

Testing the fourth Hypothesis:

For testing the fourth hypothesis which is if corporate social responsibility and / or Cybersecurity Risks, and / or Supply Chain interdependencies have no impact on SMEs Performance, the following table (7) presents multiple linear regression model depending on a cross-section data which consists of 37 companies for year 2023 to test this hypothesis.

Table (7): The multiple linear cross section regression model of the fourth hypothesis H_4

Model	*multiple Cross-section*	**Dependent variable**		Return on Investment	**VIF Test**
Independent variables	***Coefficient***	***t-ratio***	***p-value***	**Significance**	
Constant	0.696175	3.700	0.0008	**Significant at 1%**	
Corporate Social Reasonability	−0.0519977	−2.051	0.0488	**Significant at 5%**	1.349
Cybersecurity Risk	−0.0726192	−2.003	0.0539	**Significant at 10%**	1.091
Inventory Turnover	0.0856641	4.311	<0.0001	**Significant at 1%**	1.264
F-test	3.308022	***p-value***		0.025882	
Ramsey Reset test	1.47926	***p-value***		0.244	
Heterosckadicity test	9.712513	***p-value***		0.374256	
Adjusted R-squared			25.3472%		

Source: Prepared by the researcher depending on E-views software output.

From table (7) it is noted that:

1- The overall multiple linear regression model depending on a cross-section data is significant as the overall F-test for significance has a value of 3.308022 and *p-value* 0.025882 which is less than 0.05, with adjusted R-squared value of 25.3472% which means that the independent variables explain 25.3472% of the change in the Return on Investment.
2- Corporate Social Reasonability has an inverse and significant impact on Return on Investment.
3- Cybersecurity Risk has inverse and significant impact on Return on Investment.
4- Inventory Turnover has a direct and significant impact on Return on Investment.
5- There is no problem of multi-collinearity between the independent variables as the VIF test showed result less than 10 for the independent variables.
6- Ramsey reset test has a *p-value* of 0.244 which is greater than 0.05, which means that the independent variables in the models are sufficient.
7- The Heterosckadicity test has *p-values* of 0.374256, which means that the residuals have a constant variance on long run and the model does not suffer from Heterosckadicity problem.
8- The overall equation for forecasting the Return on Investment is:

$$\begin{aligned}\text{Return }\widehat{\text{on Investment}_\imath} &= 0.696175 - 0.0519977\ \text{CSR}_\text{i} \\ &- 0.0726192\ \text{Cybersecurity Risk}_\text{i} \\ &+ 0.0856641\ \text{Inventory Turnover}_\text{i}\end{aligned}$$

Therefore, the researcher will reject the null hypothesis and accept the alternative hypothesis of the fourth hypothesis which means that: Corporate Social Reasonability / or Cybersecurity Risk / or Supply Chain interdependencies (measured by Inventory

Turnover) have impact on SMEs Performance (which is measured by Return on Investment).

Conclusion:

For testing the research hypotheses, it was found that the Cross-section regression model is the most appropriate model for testing the research hypotheses, and the three cross sectional models for the research four hypotheses showed that:

1- For first hypothesis: the null hypothesis is rejected, and the alternative hypothesis is accepted, which means that there is a direct relationship between corporate social reasonability and cybersecurity perceptions.

2- For second hypothesis: the null hypothesis is rejected, and the alternative hypothesis is accepted, which means that there is a direct relationship between cybersecurity risk and supplier-customer relationship disruption.

3- For third hypothesis: the null hypothesis is rejected, and the alternative hypothesis is accepted, which means that there is an inverse relationship between cybersecurity risk and Return on Investment.

4- For fourth hypothesis: the null hypothesis is rejected, and the alternative hypothesis is accepted, which means that: Corporate Social Reasonability / or Cybersecurity Risk / or Supply Chain interdependencies (measured by Inventory Turnover) have impact on SMEs Performance (which is measured by Return on Investment).

Recommendations:

1- Adopt CSR best practices not only for the benefit of society but also as a business strategy as a mitigation against cyber-risk reactions.
2- Invest in cybersecurity since it has the spillover effect on supplier relations which can be an asset in today′s world known by scarce resources.
3- The image of SME is vital for its survival.

Future framework:

1- Use another SME performance measure rather than ROI, a performance measure that is based on cash flows rather than merely accounting income. That is because cash flow figure is what makes SME survive.
2- Incorporate other factors that affect the relation between SME and suppliers rather than cyber risk and CSR like crowding out by established firms.
3- Apply the research to listed firms that have easier access to finance.

References

Adaval, R., 2003. How good gets better and bad gets worse: Understanding the impact of affect on evaluations of known brands. *Journal of Consumer Research*, 30(3), pp.352-367.

Ambrose, M.L., Seabright, M.A. and Schminke, M., 2002. Sabotage in the workplace: the role of organizational injustice. *Organizational Behavior and Human Decision Processes*, 89(1), pp.947–965.

Arcuri, M.C., De Chiara, A. and Trubiani, C., 2017. Cyber security risk management in the financial services sector. *Journal of Financial Stability*, 32, pp.3-10.

Baggott, C. and Santos, A., 2020. The rise of cybersecurity issues for SMEs: Challenges and solutions. *Journal of Cybersecurity Studies*, 5(1), pp.11-18.

Barton, J. & Mercer, M., 2005. To blame or not to blame: Analysts' reactions to external explanations for poor financial performance. *Journal of Accounting & Economics*, 39(3), pp.509-533.

Brauer, J.R. and Tittle, C.R., 2017. When crime is not an option: inspecting the moral filtering of criminal action alternatives. *Justice Quarterly*, 34(5), pp.818–846.

Benz, R. and Chatterjee, S., 2020. Information systems security governance for SMEs: A framework for resilience. *European Journal of Information Systems*, 29(3), pp.241-256.

Binkley, M., 2021. Corporate Social Responsibility and IT Risk Management: Synergies in safeguarding information. *Journal of Enterprise Risk Management*, 14(2), pp.25-35.

Burns, A., Roberts, T.L., Posey, C., Lowry, P.B. and Fuller, B., 2023. Going beyond deterrence: a middle-range theory of motives and controls for insider computer abuse. *Information Systems Research*, 34(1), pp.342–362.

Butler, J.K. Jr. & Cantrell, R.S., 1984. A behavioral decision theory approach to modeling dyadic trust in superiors and subordinates. *Psychology Reports*, 55, pp.19-28.

Calabrese, A., Levialdi Ghiron, N. and Tiburzi, L., 2019. Cybersecurity in SMEs: an empirical analysis of factors affecting risk management strategies. *Journal of Small Business Management*, 57(2), pp.261-273.

Center for Audit Quality (CAQ), 2020. *Cybersecurity Risk Management: Insights for Investors*. [online] Available at: https://www.thecaq.org/cybersecurity-risk-management.

Chatterjee, S., 2019. Cyber risk management strategies in SMEs: A resource-based view. *Journal of Business Research*, 100, pp.503-512.

Chaiken, S., 1987. The heuristic model of persuasion. In: M.P. Zanna, J.M. Olson & C.P. Herman, eds. *Social influence: The Ontario Symposium*. pp. 3-39.

Chiu, S.-C. and Sharfman, M., 2016. Corporate social irresponsibility and executive succession: an empirical examination. *Journal of Business Ethics*, 149(3), pp.707–723.

Choi, B., Kim, S., and Jiang, Z., 2016. Remedial strategies for cybersecurity breaches: An experimental study. *Journal of Business Research*, 69(10), pp.4240-4248.

Clore, G.L. & Storbeck, J., 2006. Affect as information about liking, efficacy, and importance. In: J. Forgas, ed. *Hearts and Minds: Affective influences on social cognition and behaviour*. New York, NY: Psychology Press, pp. 123-142.

Cohen-Charash, Y. and Spector, P.E., 2001. The role of justice in organizations: a meta-analysis. *Organizational Behavior and Human Decision Processes*, 86(2), pp.278–321.

Cole, M.S., Bernerth, J.B., Walter, F. and Holt, D.T., 2010. Organizational justice and individuals' withdrawal: unlocking the influence of emotional exhaustion. *Journal of Management Studies*, 47(3), pp.367–390.

D'Arcy, J., Adjerid, I., Angst, C.M. and Glavas, A., 2020. Too good to be true: firm social performance and the risk of data breach. *Information Systems Research*, 31(4), pp.1200–1223.

Dallasega, P., Rauch, E. and Linder, C., 2018. Industry 4.0 as enabler for a sustainable development: A comprehensive review. *Journal of Cleaner Production*, 196, pp.1352-1375.

Deloitte, 2016. *The Hidden Costs of Cyber Attacks on Supply Chains*. [pdf] Available at: https://www.deloitte.com/us/en/pages/risk/articles/cyber-risk-supply-chain.html.

Dirks, K.T., Lewicki, R.J. & Zaheer, A., 2009. Repairing relationships within and between organizations: Building a conceptual foundation. *Academy of Management Review*, pp.68-84.

Du, S., Bhattacharya, C. and Sen, S., 2015. Corporate social responsibility, multi-faceted job-products, and employee outcomes. *Journal of Business Ethics*, 131, pp.319–335.

Elliott, W.B., Hodge, F.D. & Sedor, L.M., 2012. Using online video to announce a restatement: Influences on investment decisions and the mediating role of trust. *The Accounting Review*, 87(2), pp.513-535

EY, 2020. *Cybersecurity Risk: Understanding Investor Expectations*. [online] Available at: https://www.ey.com/en_gl/cybersecurity-risk-investors.

Farrell, A.M., Goh, J., and White, D., 2014. Dual processing theories in accounting research: A review and future directions. *Accounting, Organizations and Society*, 39(4), pp.195-219.

Files, R., Swanson, E.P. & Tse, S., 2009. Stealth disclosure of accounting restatements. *The Accounting Review*, 84(5), pp.1495-1520.

Frost, T.S., He, Z., HuangFu, J., and Lim, J-H., 2024. *Customer Information Technology Capability and Suppliers' Commitments*. Journal of Information Systems

Gette, M., Kryjevskaia, M., Stetzer, M. and Heron, P., 2018. The influence of dual-process theories on problem-solving. *Cognitive Science*, 42(6), pp.1805-1835.

Godfrey, P.C., Merrill, C.B. and Hansen, J.M., 2009. The relationship between corporate social responsibility and firm financial performance: a meta-analysis of experimental and survey research. *Academy of Management Journal*, 52(4), pp.743-754.

Garg, A., 2020. The impact of cybersecurity breaches on supplier financial health. *Journal of Cybersecurity*, 6(1), pp.55-69.

He, J., Frost, G. and Pinsker, R., 2020. Cybersecurity breaches and firm investment behavior. *Information Systems Research*, 31(2), pp.489-507.

Hillman, A.J., Withers, M.C. and Collins, B.J., 2009. Resource dependence theory: A review. *Journal of Management*, 35(6), pp.1404-1427.

Hoppe, G., Krämer, J. and Lutz, B., 2021. Small firm cyber risks: Strategies for prevention. *Journal of Business Continuity & Emergency Planning*, 14(1), pp.36-44.

Hovav, A. and Gray, P., 2014. The ripple effect of cyber-attacks on supply chains: A systems perspective. *Journal of Information Systems*, 28(1), pp.41-61.

Hsu, J.S.-C., Shih, S.-P., Hung, Y.W. and Lowry, P.B., 2015. The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research*, 26(2), pp.282–300.

Janakiraman, R., Lim, J. and Rishika, R., 2018. The effects of cybersecurity breaches on firm reputation and customer trust. *Journal of Marketing Research*, 55(5), pp.664-681.

Jang, S., Kim, B. and Lee, S., 2022. Impact of corporate social (ir)responsibility on volume and valence of online employee reviews: evidence from the tourism and hospitality industry. *Tourism Management*, 91.

Jafari-Sadeghi, V., Garcia-Perez, A. and Kimiagari, S., 2021. SMEs, digital transformation, and cybersecurity risk management. *Journal of Business Research*, 125, pp.261-275.

Kabanda, S., Tanner, M. and Kent, C., 2018. Exploring SMEs cybersecurity awareness and adoption in developing countries. *Computers & Security*, 78, pp.72-84.

Kadous, K., Krische, S. & Sedor, L., 2006. Using counter-explanation to limit analysts' forecast optimism. *The Accounting Review*, 81(2), pp.377-397.

Kim, S., Yin, J. and Lee, M., 2020. CSR as a tool for reputation management in cyber-risk mitigation. *Journal of Corporate Social Responsibility*, 8(3), pp.198-213.

Klein, J.G. and Dawar, N., 2004. Corporate social responsibility and consumer reactions to product harm crises. *Journal of Marketing*, 68(4), pp.245-256.

Lattanzio, P. and Ma, L., 2021. Cybersecurity breaches and supply chain innovation. *Journal of Operations Management*, 66(1), pp.114-125.

Lee, S. and Yoon, J., 2018. Does the authenticity of corporate social responsibility affect employee commitment? *Social Behavior and Personality: An International Journal*, 46(4), pp.617–632.

Liang, N., Biros, D.P. and Luse, A., 2016. An empirical validation of malicious insider characteristics. *Journal of Management Information Systems*, 33(2), pp.361–392.

Liu, H., Zhang, Y. and Wang, D., 2020. Corporate social responsibility and its insurance-like effects. *Journal of Business Ethics*, 162(2), pp.275-293.

Maasberg, M., Zhang, X., Ko, M., Miller, S.R. and Beebe, N.L., 2020. An analysis of motive and observable behavioral indicators associated with insider cyber-sabotage and other attacks. *IEEE Engineering Management Review*, 48(2), pp.151–165.

Mercer, M., 2004. How do investors assess the credibility of management's disclosures? *Accounting Horizons*, 18(3), pp.85-196.

Mitra, S. and Ransbotham, S., 2015. Information disclosure and the diffusion of information security attacks. *Information Systems Research*, 26(3), pp.565–584.

Mossburg, E., Gelinne, S. and Calzada, M., 2016. *Cyber Risk Management in Supply Chains*. Deloitte Insights. Available at: https://www2.deloitte.com/us/en/insights/topics/risk-management/cyber-supply-chain-risk.html

Muller, D., Judd, C.M. & Yzerbyt, V.Y., 2005. When moderation is mediated, and mediation is moderated. *Journal of Personality and Social Psychology*, 89(6), pp.852-863.

Onkila, T., 2015. Pride or embarrassment? Employees' emotions and corporate social responsibility. *Corporate Social Responsibility and Environmental Management*, 22(4), pp.222–236.

Perez, A. and del Bosque, I.R., 2015. How customer satisfaction influences corporate reputation and financial performance in firms. *Corporate Social Responsibility and Environmental Management*, 22(2), pp.95-109.

Pfeffer, J. and Salancik, G.R., 1978. *The External Control of Organizations: A Resource Dependence Perspective*. Harper & Row.

Ponemon Institute, 2020. *Cost of a Data Breach Report 2020*. [pdf] Available at: https://www.ibm.com/security/data-breach.

Pontari, B.A., Schlenker, B.R. & Christopher, A.N., 2002. Excuses and character: Identifying the problematic aspects of excuses. *Journal of Social and Clinical Psychology*, 21(5), pp.497-516.

Rajagopal, S., 2019. The increasing impact of cybersecurity breaches on supply chains. *Journal of Supply Chain Management*, 55(2), pp.119-134.

Ratten, V., 2019. Entrepreneurial risk management in small firms: A conceptual framework. *Small Business Economics*, 53(3), pp.611-624.

Rogers, J.L., Van Buskirk, A. & Zechman, S.L.C., 2011. Disclosure tone and shareholder litigation. *The Accounting Review*, 86(5), pp. XXX-XXX.

Sirota, D., Mischkind, L.A. and Meltzer, M.I., 2005. *The Enthusiastic Employee: How Companies Profit by Giving Workers What They Want*. Upper Saddle River, NJ: Prentice Hall.

Son, J.Y., 2011. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, 48(7), pp.296–302.

Soomro, Z.A., Shah, M.H. and Ahmed, J., 2016. Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), pp.215-225.

Tarhini, A., Hone, K. and Liu, X., 2018. Factors affecting online consumer behavior: A theoretical framework. *Journal of Retailing and Consumer Services*, 45, pp.132-140.

Walton, R., Wheeler, S., Zhang, Y. and Zhao, X., 2021. Remedial strategies in corporate cybersecurity breaches. *Journal of Corporate Finance*, 67, pp.451-466.

Wang, H., Jia, M. and Zhang, Z., 2021. Good deeds done in silence: stakeholder management and quiet giving by Chinese firms. O*rganization Science*, 32(3), pp.649–674.

Willison, R. and Warkentin, M., 2013. Beyond deterrence: an expanded view of employee computer abuse. *MIS Quarterly*, 37(1), pp.1–20.

Young, R., Zhang, L. and Prybutok, V.R., 2007. Hacking into the minds of hackers. *Information Systems Management*, 24(4), pp.281–287.

Xu, Y., Guo, J., Haislip, J.Z. and Pinsker, R., 2019. Cybersecurity disclosures and firm valuation: The role of corporate governance. *Journal of Information Systems*, 33(2), pp.107-130.

Xu, J., Yue, W.T., Leung, A.C.M., and Su, Q., 2024. *Focusing on the fundamentals? An investigation of the relationship between corporate social irresponsibility and data breach risk.* Decision Support Systems, 182.

Appendix

Variables measurements:

Corporate social responsibility and cybersecurity are measured by a questionnaire distributed among five employees working in the firms of the study sample, which consists of 37 companies listed in EGX_100 for the year 2023.

Corporate Social Reasonability CSR:	**CSR**
Firms’ policies are environment aware.	CSR_1
Firms abide by consumer protection policy.	CSR_2
Firms contribute to charity organizations.	CSR_3
Firms provide consumers with plentiful information about their activities.	CSR_4
Firms’ take part in public campaigns.	CSR_5

Cybersecurity Perception:	**CYBSP**
The organization must provide secure systems and updated software.	CYBSP_1
The organization provides cybersecurity training programs for employees.	CYBSP_2
The organization has the necessary physical resources and qualified human resources to activate cybersecurity.	CYBSP_3
There are available intruder detection programs and an execution of penetration tests.	CYBSP_4
Cybersecurity checks the integrity of the network service providers used to connect parties inside and outside the organization.	CYBSP_5

Cybersecurity Risks:	**CYSR**
There is a gap between the awareness of cybersecurity risks and the measures taken for protection.	CYSR_1
There is a potential impact of a data breach on the reputation of an organization.	CYSR_2
Third-party vendors (internet service providers) pose a significant cybersecurity risk to organizations.	CYSR_3
Emerging technologies such as artificial intelligence impact cybersecurity risks.	CYSR_4
The organization is well-prepared to respond to and recover from information security threats through cybersecurity.	CYSR_5

After distributing the questionnaire among employees, the researcher computed a weighted average mean corporate social responsibility, Cybersecurity Perception, and cybersecurity risks for each company for the year 2023.

The researcher measured supply chain by inventory turnover (INV_TO), which is the ratio between Cost of Goods Sold (COGS) and Average Inventory.

The researcher measured SME performance by computing Return on Investments (ROI) ratio.

Listed companies of sample:

```
Research Data.xlsx

One or more non-numeric variables were found.
These variables have been given numeric codes as follows.

String code table for variable 2 (Company):
  1 = 'Commercial International Bank'
  2 = 'T M G Holding'
  3 = 'El Sewedy Electric Co SAE'
  4 = 'Misr Fertilizers Production Co SAE'
  5 = 'Abu Qir Fertilizers and Chemical Industries Co SAE'
  6 = 'Alexandria Containers and goods'
  7 = 'Eastern Tobacco'
  8 = 'Qatar Natl Bank'
  9 = 'E-finance for Digital and Financial Investments'
 10 = 'Telecom Egypt'
 11 = 'Ezz Steel'
 12 = 'Egyptian Iron & Steel'
 13 = 'Emaar Misr for Development SAE'
 14 = 'EFG Hermes Holdings SAE'
 15 = 'Orascom Construction Ltd'
 16 = 'Faisal Islamic Bank of Egypt - EGP'
 17 = 'Housing & Development Bank'
 18 = 'Fawry Banking and Payment'
 19 = 'Edita Food Industries SAE'
 20 = 'Juhayna Food Industries'
 21 = 'Oriental Weavers'
 22 = 'GB AUTO'
 23 = 'Six of October Development & Invest'
 24 = 'Orascom Hotels and Development SAE'
 25 = 'Export Development Bank of Egypt'
 26 = 'Palm Hills Development Company'
 27 = 'Misr El Gadida for Housing and Development SAE'
 28 = 'Cleopatra Hospital'
 29 = 'Misr Hotels'
 30 = 'Raya Holding for Financial Investment SAE'
 31 = 'Madinet Nasr for Housing and Development SAE'
 32 = 'Al Baraka Bank Egypt'
 33 = 'Suez Canal Bank'
 34 = 'QALA For Financial Investments'
 35 = 'Obour Land for Food Industries'
 36 = 'Zahraa Maadi Investment& Development'
 37 = 'Cairo Poultry'
```

The Descriptive analysis and test of normality:

Descriptive Statistics

Variable	N	Minimum	Maximum	Mean	Std. Deviation	C.V.
CSR	37	1.00	5.00	3.75	0.92	0.24
CYBS	37	2.24	5.00	3.79	0.80	0.21
CYSR	37	2.60	5.00	4.10	0.60	0.15
INV_TO	37	0.03	1.30	0.48	0.38	0.78
ROI	37	0.06	0.64	0.24	0.15	0.62

	Shapiro-Wilk		
	Statistic	df	Sig.
CSR	.933	37	.028
CYBS	.941	37	.051
CYSR	.943	37	.057
INV_TO	.904	37	.004
ROI	.924	37	.014

The Correlation Matrix:

	CSR	CYBSP	CYSR	INV_TO	ROI
CSR	1.000				
P-value					
CYBS	0.671^{**}	1.000			
P-value	0.000				
CYSR	-0.267^{**}	-0.331^{*}	1.000		
P-value	0.000	0.045			
INV_TO	$.467^{**}$	0.674^{**}	-0.125^{**}	1.000	
P-value	0.004	0.000	0.000		
ROI	-0.184^{**}	0.101^{*}	-0.167^{**}	0.209^{**}	1.000
P-value	0.000	0.046	0.000	0.000	

Linear Regression Models:

Model 1: OLS, using observations 1-37. Dependent variable: CYBS

```
         Coefficient    Std. Error     t-ratio      p-value
const     1.37297       0.387799       3.540        0.0012      ***
CSR       0.644949      0.100633       6.409       <0.0001      ***

Mean dependent var        3.788919    S.D. dependent var     0.804873
Sum squared resid        10.72967     S.E. of regression     0.553680
R-squared                 0.139925    Adjusted R-squared     0.126780
F (1, 35)                41.07452     P-value(F)              2.24e-07
Log-likelihood          −29.59948     Akaike criterion      63.19896
Schwarz criterion        66.42080     Hannan-Quinn          64.33481
```

RESET test for specification -
Null hypothesis: specification is adequate.
Test statistic: F (2, 33) = 3.02331
with p-value = P (F(2, 33) > 3.02331) = 0.0622808

White's test for heteroskedasticity -
 Null hypothesis: heteroskedasticity not present
 Test statistic: LM = 1.78113
 with p-value = P(Chi-square (2) > 1.78113) = 0.410423

Model 2: OLS, using observations 1-37.
Dependent variable: INV_TO

	Coefficient	*Std. Error*	*t-ratio*	*p-value*	
constant	−0.705229	0.228936	−3.080	0.0040	***
CYBS	0.314070	0.0591382	5.311	<0.0001	***

Mean dependent var	0.484756	S.D. dependent var	0.378416
Sum squared resid	2.854711	S.E. of regression	0.285593
R-squared	0.146240	Adjusted R-squared	0.130419
F (1, 35)	28.20433	P-value(F)	6.26e-06
Log-likelihood	−5.104699	Akaike criterion	14.20940
Schwarz criterion	17.43123	Hannan-Quinn	15.34525

RESET test for specification -
 Null hypothesis: specification is adequate.
 Test statistic: F (2, 33) = 0.427942
 with p-value = P (F(2, 33) > 0.427942) = 0.655415

```
White's test for heteroskedasticity
OLS, using observations 1-37.
Dependent variable: uhat^2

             coefficient   std. error   t-ratio   p-value
  -------------------------------------------------------
  const        0.276619     0.348536     0.7937   0.4329
  CYBS        -0.177698     0.194023    -0.9159   0.3662
  sq_CYBS      0.0316169    0.0261120    1.211    0.2343

  Unadjusted R-squared = 0.216978

Test statistic: TR^2 = 8.028183,
with p-value = P(Chi-square (2) > 8.028183) = 0.18059
```

Model 3: OLS, using observations 1-37.
Dependent variable: ROI

```
            Coefficient   Std. Error   t-ratio    p-value
  const      0.439191     0.171494      2.561     0.0152     **
  CYSR      −0.0483444    0.0115837    −4.173    <0.0001     ***

Mean dependent var    0.241946     S.D. dependent var     0.148698
Sum squared resid     0.722199     S.E. of regression     0.147935
R-squared             0.139346     Adjusted R-squared     0.110235
F (1, 33)             4.351594     P-value(F)             0.003338
Log-likelihood        18.25119     Akaike criterion      −32.50237
Schwarz criterion    −29.39168     Hannan-Quinn          −31.42856

  RESET test for specification -
   Null hypothesis: specification is adequate.
   Test statistic: F (2, 31) = 0.254224
   with p-value = P (F(2, 31) > 0.254224) = 0.777119

  White's test for heteroskedasticity -
   Null hypothesis: heteroskedasticity not present
   Test statistic: LM = 1.91921
   with p-value = P(Chi-square (2) > 1.91921) = 0.383044
```

Model 4: Heteroskedasticity-corrected, using observations 1-37.
Dependent variable: ROI

```
              Coefficient    Std. Error    t-ratio    p-value
const          0.696175      0.188158       3.700     0.0008   ***
CSR           −0.0519977     0.0253529     −2.051     0.0488   **
CYSR          −0.0726192     0.0362480     −2.003     0.0539   *
INV_TO         0.0856641     0.0198688      4.311    <0.0001   ***
```

```
                 Statistics based on the weighted data:
Sum squared resid      99.13565   S.E. of regression    1.788274
R-squared              0.282577   Adjusted R-squared    0.253472
F (3, 31)              3.308022   P-value(F)            0.025882
Log-likelihood        −67.88282   Akaike criterion      143.7656
Schwarz criterion      149.9870   Hannan-Quinn          145.9133
```

```
Auxiliary regression for RESET specification test.
OLS, using observations 3-37 (n = 35)
Dependent variable: ROI

             coefficient    std. error    t-ratio    p-value
  ----------------------------------------------------------
  const       -0.0775214     15.1567     -0.005115   0.9960
  CSR         -0.00804930     1.40732    -0.005720   0.9955
  CYSR        -0.0141359      1.68362    -0.008396   0.9934
  INV_TO       0.0243453      2.26245     0.01076    0.9915
  yhat^2      15.3972       101.740       0.1513     0.8808
  yhat^3     -33.7829       125.081      -0.2701     0.7890

Test statistic: F = 1.479263,
with p-value = P(F (2,29) > 1.47926) = 0.244
```

```
White's test for heteroskedasticity
OLS, using observations 3-37 (n = 35)
Dependent variable: uhat^2

              coefficient   std. error   t-ratio    p-value
  ---------------------------------------------------------
  const        0.0276092    0.393306      0.07020   0.9446
  CSR          0.140630     0.117994      1.192     0.2445
  CYSR        -0.0644659    0.118840     -0.5425    0.5923
  INV_TO      -0.347043     0.165191     -2.101     0.0459  **
  sq_CSR      -0.00951695   0.00644936   -1.476     0.1525
  X2_X3       -0.0213485    0.0209632    -1.018     0.3183
  X2_X4        0.00861843   0.0260518     0.3308    0.7435
  sq_CYSR      0.0115769    0.0113399     1.021     0.3171
  X3_X4        0.0638007    0.0361237     1.766     0.0896  *
  sq_INV_TO    0.0551648    0.0555614     0.9929    0.3303

  Unadjusted R-squared = 0.277500
```

```
Test statistic: TR^2 = 9.712513,
with p-value = P(Chi-square (9) > 9.712513) = 0.374256


Variance Inflation Factors
Minimum possible value = 1.0
Values > 10.0 may indicate a collinearity problem.

         CSR    1.349
        CYSR    1.091
      INV_TO    1.264

VIF(j) = 1/ (1 - R(j)^2), where R(j) is the multiple
correlation coefficient
between variable j and the other independent variables.
```