INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN ACCOUNTING, FINANCE AND MANAGEMENT SCIENCES

OPEN ACCESS JOURNAL

Vol 14, Issue 3, (2024) E-ISSN: 2225-8329

Digital Security Risk Disclosure and Investment Process

Yap Kiew Heong, Angeline
Faculty of Business, Accounting & Economics, HELP University
Email: angeline.yap@help.edu.my

Yap Saw Teng
Faculty of Computing & Information Technology, TARC, UMT
Email: yapst@tarc.edu.my

To Link this Article: http://dx.doi.org/10.6007/IJARAFMS/v14-i3/22643 DOI:10.6007/IJARAFMS/v14-i3/22643

Published Online: 26 September 2024

Abstract

Growing interconnectedness and extensive access to cybersecurity systems increased related threats that could exploit organisations' assets. To protect the assets, organisations can implement risk mitigation measures, or transfer risks to third parties. These organisations need to disclose the digital security implemented as part of the investor relations efforts. Because of this growing cybersecurity concern, this paper examines whether investors will invest in organisations that provide the digital security risk disclosure, since it is important to assess organisations' ability to stay resilient and viable during this fast-paced technology advancement age. The researchers solicited two hundred and nineteen (219) responses from Malaysian organisations through questionnaires. Smart PLS was used to analyse the data. The results suggest that disclosure of digital security strategy, its risk mitigation, and its cyber events significantly impact the investment decision. Theoretically, this paper contributes to the literature on legitimacy theory, especially from the institutional pressure when organisations try to address the legitimacy gap during cybersecurity events. Digital security risk is growing in relevance to organisations and investors, but the current disclosure is insufficient, management should pay more attention to improving this area. Future studies may examine factors that impact digital security risks such as the role of financial implications, reputational concerns, and industry-specific regulations.

Keywords: Digital Security Disclosure, Digital Security Strategy, Digital Risk Mitigation, Cyber Events, Investment Process.

Introduction

In today's digitally driven world, organisations face an ever-increasing focus on digital security risk, necessitating a proactive approach to safeguarding sensitive information and mitigating potential threats. With the COVID-19 pandemic accelerating the shift to digital channels, the

significance of cybersecurity has been brought into sharp focus. Cybersecurity risks arise from the likelihood of threats exploiting an organisation's assets (Lim & Tan, 2020). Due to growing interconnectedness and extensive access to cybersecurity systems in recent years, information systems have become more susceptible to unintentional operator errors and either synthetic or natural calamities (Kaur, Gabriejelcic, & Klobucar, 2023). To mitigate these risks, organisations can adopt various strategies such as protecting assets, implementing risk mitigation measures, or transferring risks to third parties. Effective control implementation is based on management practices that are customised to available resources and the strength of security solutions that are matched with the organisation's business activities. It improves corporate opportunities for long-term growth and returns on investment, as well as reducing risks and ensuring knowledge security from diverse threats (Sheikhpour & Modiri, 2012). Conversely, the absence of comprehensive cybersecurity regulations leaves organisations vulnerable to security breaches and attacks on their records.

As discussed above, the present business environment pressures organisations to integrate technology into their business models, although it benefits organisations in speeding up business processes and thus boosting productivity, organisations face higher risks due to cyber threats. As part of the investor relations efforts, organisations need to increase voluntary disclosures related to digital security (Ibrahim Syed, et al., 2021; Financial Reporting Council, 2022), because investors rely on this voluntary disclosure to analyse the future of their investment. Even though cybersecurity has a significant impact on financial reporting (Heroux & Fortion, 2020; Ibrahim Syed, et al., 2021; Financial Reporting Council, 2022), past studies offered compliance guidance and directions on this emerging technology (Daud, Rasiah, George, Asirvatham, & Thangiah, 2018; Safa, Solms, & Furnell, 2016; Ifinedo, 2014; Ifinedo, 2012), organisational stock market performance after reported information technology (IT) incidences (Chai, Kim, & Rao, 2011; Hsu, Wang, & Lu, 2016; Kamiya, Kang, Kim, Milidonis, & Stulz, 2021). Most recent studies analysed the financial impact of either mandatory or voluntary disclosure on organisations' security risk management or security breaches (Goel & Shawky, 2014; Cheng, Hsu, & Wang, 2022). Little is known about the relationship between digital security and the investment process. Hence, this paper aims to expand the knowledge by investigating the factors driving the heightened focus on digital security risk disclosure and exploring their potential influence on the investment process.

The Financial Reporting Council (FRC) is promoting the use of the FRC Lab Report on Digital Security Risk Disclosure, which was recently published to address digital security risk management, and is encouraging the reporting team, risk team, and audit committees to use this Lab Report to provide voluntary disclosure. This paper contributes to several areas of the literature on digital security risk disclosure and investment process. First, this paper contributes to the body of literature by adopting the Financial Reporting Council's (2022), recommended disclosure for digital security risk disclosure. Second, this paper linked the impact of digital security strategy, its governance, risk mitigation, and cyber events (internal and external) to the investment process. Third, this paper is the first to explore the impact of digital security disclosure on investors' decisions in the Malaysian context. By enhancing an understanding of the factors influencing digital security risk and their impact on the investment process, organisations can develop effective strategies to address risks and capitalise on opportunities for growth and resilience.

This paper is organised as follows: the next section discusses the literature review to formulate hypotheses. The research method used to test the hypothesised paths of the proposed variables is presented in Section 3. The data analysis is discussed in Section 4, and the findings are elaborated in Section 5. Lastly, Section 6 concludes with implications, limitations, and recommendations.

Literature Review and Hypothesis Development

Organisational legitimacy

Organisational legitimacy or legitimacy theory branched out from the political economy theory (Rankin, et al., 2023), and it argues that organisations respond to external pressure by changing their disclosure practices as a way of maintaining their good image and conforming to investors ' expectations (D'Arcy & Basoglu, 2022). This theory suggests that organisations exist in society under an implied social contract, which emphasises that organisations must take actions to maintain legitimacy with stakeholders (Deephouse & Suchman, 2008). It refers to the extent to which an organisation's actions are approved and accepted by its stakeholders. Failing to do so shows a violation of the implied social contract, which can be destructive to the organisation's legitimacy and therefore adversely impact its existence (D'Arcy & Basoglu, 2022).

Lindblow (1993), proposed legitimacy strategies when organisation faces reputation or legitimacy challenges. Organisations should disseminate changes in their goals, methods, and behaviour to shift public expectations and show appropriate actions through education. It includes admitting mistakes, learning, and taking appropriate actions during challenging times. Benoit (1994), suggested a strategy for reputation management and image restoration, which emphasised on how organisations use disclosures to manage their reputation and image especially when facing reputation and legitimacy problems. It focuses on linguistic strategies by which legitimacy is being achieved. Benoit (1994), argues that image restoration attempts are driven by inevitable conflicts and possible reputation damage due to human acts. Reputation discourses can be targeted at the accuser, and internal and external audiences and suggest that reputation management could be driven by narcissistic desires and self-perception rather than external legitimacy or accountability.

For voluntary disclosure of digital security risk, legitimacy is acquired through certain organisational actions that are approved by its stakeholders, whereby organisations try to legitimise themselves by disseminating information that is expected of investors (Marquis, Toffel, & Zhou, 2016). A legitimacy gap will appear when organisation tries to address actions that are not in line with investors' expectations, for example, cybersecurity threats and data incidents that result in potential operational or financial impact (Financial Reporting Council, 2022; Cho & Patten, 2007). Organisational legitimacy will need to be restored and maintained through assessments, transformation, and resilience disclosures (Financial Reporting Council, 2022; Deephouse & Suchman, 2008). Digital processes and their security risk are fundamental to organisational continuity, resilience, and value creation. Disclosing such areas will provide relevant information to investors in helping them to evaluate an organisation's ability to remain feasible and resilient (Financial Reporting Council, 2022). This paper considers digital security risk disclosure as one such disclosure that is rooted in legitimacy theory and view

such disclosure as means for legitimisation, and from time to time, stakeholder expectations can change, as such organisation needs to pay unceasing attention to these expectations (D'Arcy & Basoglu, 2022).

Digital Security Risk Disclosure and Investment

To examine the digital security risk disclosure, one should first find out what drives the disclosure. Digital security risk drivers included the stakeholders, reputational, operational, and financial risk caused by cybersecurity threats such as the internal lapses that lead to most data breaches (Financial Reporting Council, 2022). It also includes the risks that arise from the process of changing a digital business model, known as digital transformation, or the increase in data reliance (Financial Reporting Council, 2022). Business continuity, resilience, and value generation are fundamentally dependent on digital systems, processes, data, and digital security (Financial Reporting Council, 2022). Several factors push the disclosure of digital security risks such as data incidents and high-profile cyber-attacks that happened recently can cause a potential impact on businesses' operations and finances (Financial Reporting Council, 2022). Digital security risks or attacks are frequently made possible because system designers made crucial assumptions about their systems' behaviour regarding digital security that unfortunately turned out to be incorrect (Halderman, 2009).

Financial Reporting Council (2022), reviewed the digital disclosures of FTSE 350 companies, discussed them with investors, and found that the cyber risk disclosures were not meeting their expectations because these companies reported standardised texts over again without making major changes to the original. Financial Reporting Council (2022), suggested that audit committees and corporate reporting teams might consider disclosing: firstly, how digital security and strategy are crucial to the organisation’s present and future business model, strategy, and environment, secondly, details of the governance processes, culture and structures build in to support digital strategy and security, thirdly, identify digital opportunities, strategy risks, and digital security that the organisation is facing currently and in the future, and lastly, highlight the impact of external and internal events and how they responded to these. In addition, organisation needs to consider the materiality and sensitivity of the disclosure and whether it is sufficient for users for decision-making.

Digital security is referred to as the capability to safeguard or defend the usage of cyberspace from cyber assaults (CNSS Secretariat, 2016). As the globe enters the era of digitalisation, cybercrime has attracted great concern from both the public and the business world. Due to the large impact cybercrime and security breaches could bring, standard setters, for example, the U.S. Securities and Exchange Commission (SEC) and Malaysia Securities Commission (SC) have provided guidelines to address and manage the accounting issues surrounding cybersecurity disclosure, governance, and management (Heroux & Fortion, 2020). In Malaysia, the outbreak of COVID-19 disease back in 2020 accelerated the development of the digital economy, and cybersecurity becoming a key factor to foster its success (Ibrahim Syed, et al., 2021). In 2014, the Malaysian Institute of Accountants (MIA) created the Integrated Reporting (IR) Steering Committee in response to the request of SC Malaysia. IR focused on five primary areas, including risk disclosure, materiality assessment, comparability and consistency, external and internal factors affecting the business, and the business value

creation model (Syed Ibrahim et al., 2021). Cybersecurity consideration and disclosure are particularly vital as it acts as a tool to demonstrate to the stakeholders the effort of a company in protecting the company from cyber threats. Hence, many organisations are changing their traditional business models to fit the digital transformation, they must rethink or improve their investment processes (Carcary & Doherty, 2016). According to Al-Ababneh, et al. (2020), it is vital to tighten control over investment processes because of the extensive trends in the development of digital technologies and the changes in the global market. The investment processes are always risky in the digital or cyber business market (Al-Ababneh, et al., 2020), therefore, the investors rely on the disclosure information to assess the prospects of the business, and the information disclosed could impact their investment intention (Ibrahim Syed, et al., 2021).

Investors go through a process to choose, assess, and manage their investment portfolios to meet their financial goals. It tries to lessen investors' risk and assists them in avoiding it. According to Cheng, Hsu, and Wang (2022), non-professional investors prioritised cybersecurity management and consider cybersecurity issues while making investment decisions. Investors would have less interest to invest in the security breached company that has disclosed the cybersecurity risk management (CSRM) report compared with the security breached company that does not disclose the CSRM report (Cheng, Hsu, & Wang, 2022). Investors' interest in the investment process will decline following the disclosure of a cybersecurity breach may vary depending on whether the organisation previously informed investors of its strategic cybersecurity risk management measures. Initiatives for managing cybersecurity risks strategically should show that management is aware of those risks and has taken action to address them (Demek & Kaplan, 2023). Investors may, for instance, be more likely to attribute the external forces that are beyond the organisation's control to the breach, such as hackers (Demek & Kaplan, 2023). For organisations that indicate strategic risk management initiatives, a CEO's apology after a cybersecurity breach positively affects impressions and perceptions of CEO cognitive trust and affective. Moreover, when the CEO does not issue an apology, it lowers their investors' investment interest. In contrast, letting investors know about earlier strategic cybersecurity risk management activities could make them more wary of a compromise. However, businesses must provide investors with more information about their cybersecurity to assist the investors in their investment process (D'Arcy & Basoglu, 2022).

Few other studies examined organisational stock market performance after announced information technology breaches and incidences (Campbell, Gordon, Loeb, & Zhou, 2003; Cavusoglu, Mishra, & Raghunathan, 2004; Goel & Shawky, 2014). They found an unfavourable market response when an organisation reported cybersecurity breach incidents. A more recent study by Kamiya, Kang, Kim, Milidonis, and Stulz (2021), found that breaches with personal financial information loss are seen as negative information about the security risk toward breached organisations by their competitors, and their stakeholders. In contrast, the study by Chai, Kim, and Rao (2011), shows favourable responses from investors to an organisation's security investment decisions. Gordon and Loeb (2002), found that information security disclosures are positively and significantly related to market value. This paper expands the literature by adopting the Financial Reporting Council's (2022), recommended

disclosure for digital security risk disclosure, and links it to the investment process in the Malaysian context.

Strategy

Leitner & Guldenberg (2010), defined strategy as a plan or pattern that combines an organisation's main objective, policies, and sequence of action, aiming to achieve the organisation's intended goal and objective effectively. Rowe and Gallaher (2006) categorised cybersecurity strategies into proactive and reactive approaches. A proactive cyber security strategy involves anticipating security compromises and incorporating safeguards into the IT system to prevent them. A reactive cyber security strategy involves responding to known threats with established technologies to address security compromises effectively and efficiently. In general, adopting a proactive strategy can result in fewer cybersecurity breaches, while adopting a reactive strategy can be more cost-efficient. They also stated that both internal and external information resources influence the strategy adopted by each organisation in approaching cyber security investment decisions. For example, when an organisation has greater availability of information, it is more likely to adopt proactive rather than reactive cyber security strategies.

Investors want relevant digital strategy disclosures that give the context for digital strategy and security and its importance to the organisation's business model and ability to add value. It should show how external trends related to digital strategy and security and how it integrated or linked to the corporate approach (Financial Reporting Council, 2022). However, Riaz, Hunjra, and Azam (2012), stated that investors usually relied more on their instincts and emotions rather than strategy when making investment decisions. In contrast, Omotayo, Oladipo, and Olusegun (2020), argued that corporate strategy has a positive and significant relationship impact on investment decisions. They emphasised that an organisation should implement a comprehensive strategic plan for any investment decision to achieve its set goals. Based on the discussion above, the researchers propose the following hypothesis**:**

H_1: There is a positive and significant relationship between strategy and the investment process.

Governance

Understanding risk is about understanding how the external environment affects an organisation and how the organisation responds and mitigates those risks (Financial Reporting Council, 2022). The Council criticised FTSE 350 companies often covering "what" is governance but neglecting "why" and "how" are governance likes. They argued the companies should focus on a more integrated approach to digital security and strategy governance which gives a clear link between a wider internal and external stakeholder setting. Investors seek governance disclosures that link the digital transformation governance and security risks to strategy and risk appetite. Organisations must establish reporting lines, procedures, and channels of communication, take cybersecurity into account, then monitor performance, and appoint cybersecurity experts (Sutherland, 2018). They can promote a comprehensive and active strategy for handling cybersecurity risks and coordinating

cybersecurity practices with organisational goals by connecting cybersecurity to governance (Eugen & PetruÅ£, 2018). Board members should have oversight of cybersecurity risks and identify ownership of specific risks, then take necessary steps to foster a digital security culture, in addition, the board should set criteria and obtain assurance for their skills and abilities (Financial Reporting Council, 2022).

Public listed organisations ought to make disclosures of material information in the form of mandatory or voluntary disclosure. While organisations' investment in cybersecurity strategy is essential, it is crucial to disclose controls and incorporate cybersecurity management in the corporate governance structure (Peng & Krivacek, 2020). Cybersecurity governance is corporate governance detailing the management and control of cybersecurity issues. Part of information security governance includes cybersecurity governance which is referred to as the process of guiding and supervising the protection of a company's digital properties against threats associated with Internet use (von Solms & von Solms, 2018). According to Ernst and Young LLP (2020), investors are interested in understanding whether the board members were involved in cybersecurity supervision, sharing the responsibility with audit, risk, and technology committees, or establishing an exclusive cybersecurity reporting and risk disclosure team. Stakeholders are concerned about how organisation prepare for and respond to cybersecurity incidents (Ernst & Young LLP, 2020). Cybersecurity governance outlines how the board's oversight of these critical risk management efforts is said to be critical to investors (Ernst & Young LLP, 2020). Hsu, Lee, and Straub (2012), found that corporate security governance effectively decreases vulnerability to cyber-attacks which will reduce huge financial losses. Therefore, cybersecurity governance could decrease investment risk and increase investors' investment intentions. Based on the above discussions for cybersecurity governance, the researchers propose:

H_2: There is a positive and significant relationship between governance and the investment process.

Risk Mitigation

According to Dang, Phan, Nguyen, and Hoang (2020), risk can be perceived as a necessary evil that should be mitigated or minimised in the best possible way. From an organisation's perspective, the risk is present due to uncertain events and circumstances, which may lead to the organisation suffering from losses such as financial loss, performance loss, material loss, and time loss (Al-Abrrow, Alnoor, & Abbas, 2019). Institutional investors seek to understand an organisation's resilience to risks in assessing its capacity to deal with them and capitalise on potential opportunities (Financial Reporting Council, 2022). Thus, organisations that proactively disclose their risk management practices stand to gain more benefits. Financial Reporting Council (2022), argued that while controls, procedures, and processes are crucial to managing risk, nurturing a strong corporate culture in cyber is equally crucial, and it is inseparably connected to achievement and performance. Top management plays an important role in setting the organisation's culture. Transparent communication within the organisation is essential to cultivate the growth of a positive organisational culture. A positive culture pushes rules or procedures to be changed into organisational awareness and actions. Culture itself can be an effective risk mitigation tool. Nurturing a culture that emphasises

security encourages all stakeholders to appreciate its contribution. Then, they can give confidence to the functioning of top management within the existing governance structures in assisting them to mitigate risk (Financial Reporting Council, 2022).

The risk of a cybersecurity breach affects the organisation's operations in the virtual environment (Uddin, Ali, & Hassan, 2020). It is because loopholes in cyberinfrastructure create opportunities for hackers to infiltrate the organisation's network to disrupt operations. Simon and Omar (2020), highlighted that cyberattacks significantly affect the supply chain as cyberattacks disrupt supplier production schedules and logistic industry deliveries. To effectively manage cyber risks, organisations must make investments in cybersecurity measures. Mazzoccoli and Naldi (2022), stated that if the organisation does not invest money in security, the vulnerability of a system will increase over time as new threats are created and the shielding capability of the protection tools in place degrades. Hence, they argued that organisations should continue investing in security to effectively counter new threats and mitigate the risk of data breaches. Bodin, Gordon, Loeb, and Wang (2018), suggested that in addition to investing in activities that mitigate cybersecurity risks such as firewalls and intrusion detection systems, organisations can consider investing in cybersecurity insurance to transfer some of the risk associated with potential cybersecurity breaches. However, Nguyen and Dong (2013), discovered that higher business risks lead to fewer investment activities. Higher risks can create greater uncertainty and the possibility of incurring losses, causing some organisations to choose to reduce investment activities to protect their financial stability. Based on the above arguments, the researchers propose the following hypothesis:

H_3: There is a positive relationship between risk mitigation and the investment process.

Cyber Events

A cybersecurity event is the disturbance of a data system or unauthorised access to, acquisition of, and use of non-public information (Allodi & Massacci, 2017). Organisations are confronted by many external and internal digital security events that will adversely affect their strategy, governance structures, and risk management. They must invest in cyber security to safeguard information and keep up with new threats. To tackle threats to cybersecurity during an event, event organisers, staff, and participants should be educated on best cybersecurity practices (Allodi & Massacci, 2017). Prioritising cybersecurity during event planning is crucial, as is putting in place the necessary safeguards to make sure that everyone who attends is safe and secure. It is crucial to implement monitoring and detection systems, mobile device security, and post-event evaluation (Bartock, et al., 2016) to guarantee a safe and secure environment for all participants.

Investors are interested to know whether the organisation has effectively responded to cyber events and learned from them by incorporating improvements to relevant structures and processes (Financial Reporting Council, 2022). When a cyber-attack happens, investors are concerned whether the organisation provides meaningful details on the event's nature, and whether actions are taken or to be taken immediately and forecast the event's impact. Proactive actions will assist the organisation in controlling the narrative and giving relevant details directly to stakeholders. From the legitimacy perspective, organisations that exist in

society must act to maintain legitimacy before their stakeholders (Deephouse & Suchman, 2008; Suchman, 1995). In the context of cybersecurity disclosure, this theory suggests that when a cybersecurity incident occurs, organisations should respond quickly to the breach and disclose the incident to address the resulting legitimacy gap (D'Arcy & Basoglu, 2022).

Previous research has indicated that cybersecurity events, such as software vulnerabilities (Telang & Wattal, 2007) and cybersecurity breaches cause unfavourable market reactions (Cheng & Walton, 2019; Amir, Levi, & Livne, 2018). Wang, Kannan, and Ulmer (2013) argue that disclosures regarding security breaches may influence the judgement of investors of the violated organisation's business value. However, an organisation's disclosure of cybersecurity incidents and its response to them can reduce investors' concern and distrust of the organisation due to the incident (Demek & Kaplan, 2023), especially apologies by the chief executive officer (CEO) positively influencing investors' perceptions and increasing their trust in CEO. Hence, the hypothesis is formed as follows:

H_4: There is a positive relationship between cyber events and the investment process.

Methodology

Research Design

Sampling

This paper employed a quantitative research approach. According to Sekaran and Bougie (2016), by conducting primary data research, data is found first-hand, which was carried out independently by the researcher, either through open-ended interviews or structured questionnaires. To test the above hypotheses, survey questionnaires in Google Forms were used to gather data more efficiently. The questionnaires were distributed using emails and other social media platforms such as WhatsApp, Messenger, and Instagram. The distributions received two hundred and forty-five (245) respondents, however, after the data cleaning process, the researchers removed questionnaires that were not suitable, hence, the sample size was reduced to two hundred and nineteen (219) respondents.

Instrument

The questionnaire is divided into six (6) sections. Section One (1) to Section Five (5) are questions related to the variables. The first part focused on statements related to strategy, followed by governance, risk mitigation, and cyber events; Section 5 included statements related to the investment process. These sections asked the respondents to rate twenty-three (23) statements using a 7-point Likert scale (1 = never, 2 = rarely, 3 = occasionally, 4 = sometimes, 5 = frequently, 6 = usually, and 7 = every time). All statements in Section One (1) to Four (4) were adapted from a digital security disclosure lab report issued by the Financial Reporting Council (2022), while the statements on the investment process (Section 5) were adapted from Duuren, Plantinga, and Scholtens (2016). The researchers carried out a reliability test using Cronbach's Alpha. All the variables' reliability test results met the minimum acceptable value of 0.7 for Cronbach's Alpha (Taber, 2018; Cronbach, 1951). The last Section solicited the profile of respondents which is presented in Table 1. It showed that 32.9 percent of the respondents were from financial services, followed by 16 percent from products/services and 12.3 percent from technology, telecommunication/media. In terms of

annual sales in million, 30.6 percent of the respondents generated less than RM 20 million annually, 13.7 percent and 12.8 percent generated more than RM 50 million to RM 100 million, and more than RM 300 million to RM 400 million annually, respectively. 31.1 percent of these respondents have been in operation for less than 5 years, followed by 25 percent operating for more than 16 years and 22.4 percent for between 11 to 15 years.

Table 1
Demographic Of The Respondents

Demographic	Frequency	Percentage
Industry		
Construction	7	3.2
Products/services	35	16.0
Energy & utilities	4	1.8
Financial services	72	32.9
Health care	21	9.6
Industrial products/services	26	11.9
Plantations	4	1.8
Property & REIT	14	6.4
Technology, telecommunication/media	27	12.3
Transport	9	4.1
Average annual sales in millions of RM		
≤ 20	67	30.6
> 20 - 50	24	11.0
> 50 - 100	30	13.7
> 100 - 200	18	8.2
> 200 - 300	26	11.9
> 300 - 400	28	12.8
> 400 - 500	9	4.1
> 500	17	7.7
Number of years in operation		
≤ 5	68	31.1
6 - 10	47	21.5
11 - 15	49	22.4
≥ 16	55	25.0

Data Analysis

This paper used structural equation modelling to analyse the measurement and structural, a two steps approach recommended by (Anderson and Gerbing 1988). The first step is a convergent validity and discriminant validity for model measurement, followed by the second step which is a structural model analysis for hypotheses testing.

Measurement Model

Smart PLS data analysis involved the assessment of internal consistency reliability, outer loadings, convergent validity, and discriminant validity was performed on the above data (Hair, Hult, Ringle, & Sarstedt, 2022)

The researchers performed a measurement model analysis comprising six constructs. As shown in Table 2, all constructs reported outer loadings, composite reliability, and AVE of more than 0.5, which were acceptable (Hair, Hult, Ringle, & Sarstedt, 2022).

Table 2
Convergent Validit

Constructs	Outer Loadings	Composite Reliability	AVE
Strategy (ST)		0.822	0.724
ST1	0.884		
ST2	0.887		
ST3	0.776		
Governance (GN)		0.813	0.628
GN1	0.774		
GN2	0.718		
GN3	0.824		
GN4	0.847		
Risk mitigation (RM)		0.867	0.708
RM1	0.844		
RM2	0.806		
RM3	0.880		
RM4	0.833		
Cyber Events (CE)		0.902	0.667
CE1	0.777		
CE2	0.867		
CE3	0.820		
CE4	0.822		
CE5	0.766		
CE6	0.842		
Investment Process (IP)		0.897	0.656
IP1	0.770		
IP2	0.809		
IP3	0.842		
IP4	0.805		
IP5	0.821		
IP6	0.811		

Discriminant validity measures to what extent the constructs examined are genuinely distinct from one another. Henseler, Ringle and Sarstedt (2015) argue that HTMT was able to obtain

higher specificity based on different loading values and sample size. As shown in Table 3, all values are lower than the required threshold value of 0.9 providing support for the measures' validity (Henseler, Ringle, & Sarstedt, 2015, Hair, Hult, Ringle, & Sarstedt, 2022).

Table 3
HTMT Ratio Result

	ST	GN	RM	CE	IP
Strategy (ST)	0.851				
Governance (GN)	0.717	0.792			
Risk mitigation (RM)	0.729	0.800	0.841		
Cyber events (CE)	0.658	0.692	0.748	0.817	
Investment process (IP)	0.672	0.697	0.740	0.712	0.810

From the above measurement model results, it is found that all the constructs have obtained substantial reliability and validity. The model is expected to be acceptable for the model testing in the next section.

Model Testing

Having considered reliability and validity of the constructs, the researchers performed bootstrapping procedure under SmartPLS to test the significance of the path analysis and to process its coefficients. The bootstrapping procedure created 5,000 resample to estimate path analysis and to test the hypotheses developed (Said, Abdul Jalil, & Zainal, 2023; Abdul Kalid, Jabar, Aidil Hasim, & Jamaris, 2020). The R-square of the investment process (IP) is 0.631, which is above the threshold value of 0.333 indicating a moderate model (Khalid , Jabar, Hashim, & Jamaris, 2020). Then, a path coefficient was performed to test the strength of relationships between the variables.

The path coefficient value of 0.170 and p-value < 0.05 for H1 showed that strategy (ST) has significant impact on investment process (IP). In addition, the results for H3 and H4 also showed that risk mitigation (RM) (p-value < 0.01) and cyber events (CE) (p-value < 0.01) positively impacted the investment process, respectively. However, H2 governance (GN) (p-value > 0.05) did not impact the investment process (IP). Hence, H1, H3 and H4 are supported.

Table 4
Hypothesis Result

Paths	Path coefficients	T-value	P-value	Results	(f2)
Strategy -> Investment Process	0.170	2.006	0.045	Supported	0.032
Governance -> Investment Process	0.154	1.678	0.093	Not supported	0.020
Risk mitigation -> Investment Process	0.281	3.697	0.000	Supported	0.057
Cyber events -> Investment Process	0.283	3.589	0.000	Supported	0.087

Discussion

Legitimacy theory advocates that organisation exists must act according to the social expectation to maintain legitimacy (Deephouse & Suchman, 2008). Table 4 presented the

hypotheses results; it was found strategy (ST) is positively significantly related *(p-value 0.045 < 0.05)* to investment process (IP). This is consistent with the argument by Heroux and Fortion (2020), and Ibrahim Syed, et al (2021), that digital disclosures can assist investors and stakeholders to have more insights about organisations' digital strategy during investment analysis. If organisation does not disclose any cybersecurity strategies and measures to overcome risks and threats, it will give negative signals to investors about the sustainability of business prospects especially the threat and risks of cybersecurity issues faced by organisations (Ibrahim et al., 2021). This positive significant finding is also supported by previous research (Deloitte, 2023; Blackburn, Galvin, Laberge, & Williams, 2021 and Koch & Windsperger, 2017) as it was found that organisations with well-defined digital strategies tend to attract more investment due to their perceived competitive advantage. It also serves to address and mitigate cybersecurity risk effectively, making it more appealing to potential and current investors (Eijkelenboom & Nieuwesteeg, 2021; Calderon & Gao, 2020 and Berkman, Jona, Lee, & Soderstrom, 2018). This implies that organisations that effectively align their digital security strategies with their broader business goals are more likely to receive favourable investment decisions. As such, organisations should prioritise their strategic alignment and effectively communicate their digital security to attract investment.

Table 4 reported significant positive relationship between risk mitigation *(p-value = 0.000 < 0.01)* and investment process (H3). Consistent with this result, other studies also supported similar finding as a strong risk management plan (Duvenhage, Smit, & Botha, 2022) and risk management framework (Yang, Lau, & Gan, 2020) led to transparent reporting and thus increased investors' willingness to invest in those organisations. According to Maricela, Lazaro, Maria, and Vartika (2022), cyber risk management disclosures should be strengthened to gain investors' confidence on organisational strategy in managing and monitoring digital risks. Legitimacy theory suggests that an organisation can repair, maintain, and gain legitimacy should the social contract breakdown. Past legitimacy studies provided evidence of how level of disclosure differs when organisations responded to certain events in view of reputation (Buhr, 1998; Bebbington, Larrinaga, & Moneva, 2008). However, lack of updated information related to risk management plans will give negative perception to investors who are searching and determining riskiness of organisation after cyber incidents occurred (D'Arcy & Basoglu, 2022). Organisations that disclosing cyber risks can mitigate negative market reactions in response to subsequent security breaches (Wang, Kannan, & Ulmer, 2013). The Financial Reporting Council (2022), added that investors demand disclosures that provide an understanding of the relationship between strategic objectives, risk appetite, and the management of specific risks. This allows investors to assess risk management alignment and ownership structures' effectiveness in achieving strategic goals including investment process.

Cyber events (H4) is another factor which is also positively and significantly related to (*p value = 0.000, < 0.01)* investment process. This finding is supported by Cheng, Hsu, and Wang (2022), that the investors are expected to know whether the company has done effective management on the occurrence of cybersecurity incidents such as security breaches to make further investment decisions. When an organisation discloses cyber incidents, the related costs and effect due to the cyber incidents should be reported in the interest of stakeholders and investors (Bakker, 2015). If the organisation encountered security breaches and did not

provide any prior information on how they manage cybersecurity risk effectively, it will affect the investment judgement (Cheng, Hsu, & Wang, 2022).

Legitimacy theory suggests that when a cybersecurity incident occurs, organisations should respond quickly to the breach and disclose the incident to address the resulting legitimacy gap (D'Arcy & Basoglu, 2022). Stakeholders emphasised on the significance of cyber incident disclosures due to the increasing number of security breaches (Chen, Henry, & Jiang, 2022). They suggest that regardless of the severity of the security breach, investors penalise breached organisations for subsequently decreasing cyber incident disclosures. Openly communicating about a cybersecurity event and steps taken to address the situation can foster transparency and trust among investors, reducing investor concern due to the event (Demek & Kaplan, 2023). Therefore, disclosing cybersecurity events can positively influence the investment process.

Allodi and Massacci (2017), argued that event organisers, staff, and participants should be educated on best cybersecurity practices. It is essential to give cybersecurity top priority when arranging an event and to put the appropriate security measures in place to ensure that everyone who attends is safe. It is also critical to incorporate monitoring and detection systems, mobile device security, and post-event evaluation to ensure a secure environment for all participants. According to the Financial Reporting Council (2022), organisations normally rely on safety surveillance systems, threat information, and incident-management protocols to identify, evaluate and appropriately handle these events. Most investors would want to know how well an organisation reacts to a cybersecurity problem, particularly in times of political unrest.

Conclusion

With the rapid growth of the digital era and the digitisation of business, it gives rise to cybersecurity issues that affect investor confidence and trust in organisations. This paper considers the factors that drive a greater focus on digital security risk and examines the relationship between four factors (strategy, governance, risk mitigation, and cyber events) and the investment process. The results showed that strategy (H1), risk mitigation (H3) and cyber events (H4) are positively and significantly related to the investment process. Therefore, organisations should consider these aspects when making plans relating to cybersecurity. This paper contributes to the literature on digital security factors and their influence on the investment process from the institutional perspective and propose that organisations or investors from different industries to consider cyber events before the investment decisions, because ignoring such cyber breaches from the cybersecurity event will harm the organisations in the short term and long term.

To enhance cybersecurity in the investment process and external cyber reporting capabilities, several actions can be taken. Organisations can identify the digital security risks that they are potentially facing now and, in the future, and take suitable actions to respond to these issues (Financial Reporting Council, 2022). Next, organisations can set out the appropriate business models or approaches to handle those internal and external digital factors (Financial Reporting Council, 2022). Furthermore, reference surveys can be conducted in organisations, where they cross-check their strategic objectives with the risk appetite and then provide

information that regards mitigations of those risks (Financial Reporting Council, 2022). Organisations can also examine the nature of the incidents that happened and take immediate actions to reduce the impacts on the investment (Financial Reporting Council, 2022).

The government plays an important role in creating awareness of cybersecurity by offering and conducting training for the employees on the importance of cybersecurity. The government can also give grants to encourage organisations to strengthen workplace cybersecurity. Responding to stakeholders' demand for more information from organisational cybersecurity, the MASB may consider issuing an assurance framework and voluntary reporting as a way for organisation to disseminate their cybersecurity risk management strategies to interested stakeholders. The reporting can include a narrative description of the organisation's cybersecurity risk management program, management's claims as to the description's adherence to the guidelines outlined by the MASB, and whether the cybersecurity controls were executed efficiently and effectively during the reporting period.

To enhance investor confidence and trust, organisations may consider the following cybersecurity recommendations. First, organisation should raise cybersecurity awareness by involving some management team members or employees in conferences that address recent cybersecurity trends and issues. This will enable organisation to identify potential risks, proactively prepare solutions, and mitigate the severe impacts of cybersecurity incidents. Next, organisation can also provide cybersecurity training to employees to increase their cybersecurity awareness. These can prepare the organisation for preventing and responding to cybersecurity incidents to foster investor confidence and trust. Besides, organisation should voluntarily disclose cybersecurity information, including incident details, lessons learned, and strategies for future improvements. This transparency can boost investor confidence and trust in the organisation. Furthermore, organisation should emphasise cybersecurity investments, such as regular IT software upgrades and scheduled maintenance, to enhance cybersecurity and reduce cyber risks.

There are limitations in this paper, including the sample size is not too large, readers should be prudent while interpreting and generalising the results of this paper. Moreover, to eliminate sampling biases, future studies might consider gathering data from a larger sample size and include secondary sources to improve the representativeness and comprehensiveness of the results. Organisations may benefit from knowledge in this area by strengthening their digital and business viability and resilience, in addition, to making the appropriate investment decisions. Future studies may also delve into the factors that impact the disclosure of cybersecurity breaches or incidents within an organisation. This could involve examining the role of financial implications, reputational concerns, and industry-specific laws and regulations. By exploring these aspects, valuable insight can be gained regarding the barriers and motivation for disclosing cybersecurity incidents. For instance, an analysis of the tensions between privacy, the ethical obligations of stakeholders, and potential ethical dilemmas faced during the disclosure process should be undertaken. By addressing these areas, future studies can contribute to a comprehensive understanding of cybersecurity disclosure and investment processes.

References

Kalid, F., Jabar, J., Hasim, A. M., & Jamaris, N. W. (2020). What Tickles Your Fancy? The Case of Technology and Engineering Students Becoming Entrepreneurs. *Asian Journal of Business and Accounting 13(1)*, 263-287.

Al-Ababneh, H. A., Al-Qudah, O. M., Amoush, A. H., Popova, S., Popova, O., Tomashevskaya, E. (2020). Risks of Investment in Digital Marketing: The Optimum or Minimum? *Journal of Critical Reviews, 7(13)*, 2897-2907.

Al-Abrrow, H., Alnoor, A., & Abbas, S. (2019). The Effect of Organizational Resilience and CEO's Narcissism on Project Success: Organizational Risk as Mediating Variable. *Organization Management Journal, 16(1)*, 1-13.

Allodi, L., & Massacci, F. (2017). Security Events and Vulnerability Data for Cybersecurity Risk Estimation. *Risk Analysis An International Journal, 37(8)*, 1606-1627.

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies, 23(3)(11)*, 1177-1206.

Bakker, T. G. (2015). *Accuracy of Self-Disclosed Cybersecurity Risks of Large US Banks* . Madison, South Dakota: Dakota State University .

Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witt, G., & Scarfone, K. (2016). *Guide for Cybersecurity Event Recovery.* Gaithersburg: National Institute of Standards and Technology.

Bebbington, J., Larrinaga, C., & Moneva, J. M. (2008). Corporate social reporting and reputation risk management. *Accounting, Auditing & Accountability Journal, 21(3)*, 337-361.

Benoit, W. L. (5 December, 1994). Accounts, excuses, and apologies : a theory of image restoration strategies. *State University of New York Press*, p. 197.

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy, 37(6)*, 508-526.

Blackburn, S., Galvin, J., Laberge, L., & Williams, E. (8 October, 2021). A winning digital strategy requires new twists to familiar moves. *Strategy for a digital world*, pp. 1-11.

Bodin, L. D., Gordon, L. A., Loeb, M. P., & Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy, 37(6)*, 527-544.

Buhr, N. (1998). Environmental performance, legislation and annual report disclosure: the case of acid rain and Falconbridge. *Accounting, Auditing & Accountability Journal, 11(2)*, 163-190.

Calderon, T. G., & Gao, L. (2020). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. *International Journal of Auditing, 25(1)*, 24-39.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer SecurityVolume, 11(3)*, 431-448.

Carcary, M., & Doherty, E. (2016). The Digital Wild West: Managing the Risks of Digital Disruption. *The European Conference on Information Systems Management* (pp. 29-36). Reading: Academic Conferences International Limited.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce, 9(1)*, 69-104.

Chai, S., Kim, M., & Rao, R. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems, 50*, 651-661.

Chen, J., Henry, E., & Jiang, X. (2022). Is Cybersecurity Risk Factor Disclosure Informative? Evidence from Disclosures Following a Data Breach. *Journal of Business Ethics, 187*, 199–224.

Cheng, X., & Walton, S. (2019). Do nonprofessional investors care about how and when data breaches are disclosed? *Journal of Information Systems, 33(3)* , 163-182.

Cheng, X., Hsu, C., & Wang, T. (2022). Talk too much? The Impact of Cybersecurity Disclosures on Investment Decisions. *Communications of the Association for Information Systems, 50*, 481-500.

Cho, C. H., & Patten, D. M. (2007). The role of environmental disclosures as tools of legitimacy: A research note. *Accounting, Organizations and Society, 32(7-8)*, 639-647.

CNSS Secretariat. (2016). *CNSS Annual Report 2015/2016.* Fort George G. Meade: National Security Agency.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*, 297–334.

Dang, H. T., Phan, D. T., Nguyen, H. T., & Hoang, L. H. (2020). Factors Affecting Financial Risk: Evidence from Listed Enterprises in Vietnam. *Journal of Asian Finance, Economics and Business, 7(9)* , 11-18.

D'Arcy, J., & Basoglu, A. (2022). The Influences of Public and Institutional Pressure on Firms' Cybersecurity Disclosures. *Journal of the Association for Information Systems, 23(3)*, 779-805.

Daud, M., Rasiah, R., George, M., Asirvatham, D., & Thangiah, G. (2018). Bridging the Gap Between Organisational Practices & Cyber Security Compliance: Can Cooperation Promote Compliance In Organisations? *International Journal of Business and Society, 19 (1)*, 161-180.

Deephouse, D. L., & Suchman, M. (2008). Legitimacy in Organizational Institutionalism. In *The SAGE Handbook Of Organisational Institutionalism* (pp. 49-77). SAGE Publications Ltd.

Deloitte . (2023). *Unleashing value from digital transformation: Paths and pitfalls.* UK: Deloitte Touche Tohmatsu Limited.

Demek, K. C., & Kaplan, S. E. (2023). Cybersecurity breaches and investors' interest in the firm as an investment. *International Journal of Accounting Information Systems, 49*, 100616.

Duuren, E. v., Plantinga, A., & Scholtens, B. (2016). ESG Integration and the Investment Management Process:. *Journal of Business Ethics,138*, 525–533.

Duvenhage, F., Smit, A., & Botha, M. (2022). Cyber Security disclosure in the banking sector: A case of South Africa and China. *31st International Biometric Conference.* Riga: International Biometric Society.

Eijkelenboom, E. V., & Nieuwesteeg, B. F. (2021). An analysis of cybersecurity in Dutch annual reports of listed companies. *Computer Law & Security Review, 40*.

Ernst & Young LLP. (2020). *What companies are disclosing about cybersecurity risk and oversight in 2020.* US: Ernst & Young Global Limited.

Eugen, P., & PetruÅ£, D. (2018). Exploring the New Era of Cybersecurity Governance. *Ovidius University Annals, Economic Sciences Series, 1*, 358-363.

Financial Reporting Council. (2022). *FRC Lab Report: Digital Security Risk Disclosure.* London: The Financial Reporting Council Ltd.

Goel, S., & Shawky, H. A. (2014). The Impact of Federal and State Notification Laws on Security Breach Announcements. *Communications of the Association for Information Systems, 34(1)*, 37-50.

Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security, 5(4)*, 438-457.

Hair, J. F., Hult, G. M., Ringle, C. M., & Sarstedt, M. (2022). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), 3rd Edition.* Thousand Oaks, CA: Sage.

Halderman, J. A. (2009). *Investigating security failures and their causes: An analytic approach to computer security.* Princeton University.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science 43*, 115–135.

Heroux, S., & Fortion, A. (2020). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives, 19(2)*, 73-100.

Hsu, C., Lee, J. N., & Straub, D. W. (2012). Institutional Influences on Information Systems Security Innovations. *Information Systems Research, 23(2)*.

Hsu, C., Wang, T., & Lu, A. (2016). The Impact of ISO 27001 Certification on Firm Performance. *49th Hawaii International Conference on System Sciences (HICSS)* (pp. 4842-4848). Koloa: IEEE COMPUTER SOCIETY.

Ibrahim, N. S., Shamsudin, A., Abdullah, S., Ibrahim, M. T., Jaaffar, M. Y., & Bani, H. (2021). Content Analysis of Voluntary Disclosures on Cybersecurity in Malaysia. *International Journal of Academic Research in Accounting Finance and Management Sciences, 11(4)*, 10-28.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31 (1)*, 83-95.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51(1)*, 69-79.

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.

Kaur, R., Gabriejelcic, D., & Klobucar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion, 97*, 101804.

Khalid , F. A., Jabar, J., Hashim, M. A., & Jamaris, N. W. (2020). What Tickles Your Fancy? The Case of Technology and Engineering Students Becoming Entrepreneurs. *Asian Journal of Business and Accounting, 13(1)*, 263-287.

Koch, T., & Windsperger, J. (2017). Seeing through the network: Competitive advantage in the digital economy. *Journal of Organisation Design 6(6)*, 1-30.

Leitner, K.-H., & Guldenberg, S. (2010). Generic strategies and firm performance in SMEs: a longitudinal study of Austrian SMEs. *Small Business Economies, 35*, 169-189.

Lim, C. C., & Tan, S. S. (2020). The Significance of Personal Value, Risk Attitude and Trust on Life Insurance Ownership in the Northern Regions of Malaysia. *Jurnal Pengurusan, 58*, 67–78.

Lindblow, C. K. (1993). The Implications of Organisational Legitimacy for Corporate Social Performance and Disclosure. *Critical Perspectives on Accounting Conference.* New York.

Maricela, R., Lazaro, R. A., Maria, E. G., & Vartika. (2022). The Disclosures of Information on Cybersecurity in Listed Companies in Latin America—Proposal for a Cybersecurity Disclosure Index. *Sustainability, MDPI, 14(3)*, 1.

Marquis, C., Toffel, M. W., & Zhou, Y. (2016). Scrutiny, Norms, and Selective Disclosure: A Global Study of Greenwashing. *Organization Science, 27(2)*, 483–504.

Mazzoccoli, A., & Naldi, M. (2022). Optimizing Cybersecurity Investments over Time. *Algorithms, 15(6)*, 121.

Nguyen, P. D., & Dong, P. T. (2013). Determinants of Corporate Investment Decisions: The Case of Vietnam. *Journal of Economics and Development, 15(1)*, 32-48.

Omotayo, E. O., Oladipo, O. N., & Olusegun, E. A. (2020). Impact of Corporate Strategy on Investment Decision in Nigeria. *Acta Universitatis Danubius, 16(5)*, 285-302.

Peng, J., & Krivacek, G. (2020). The Growing Role of Cybersecurity Disclosures. *ISACA Journal, 1*, 1-7.

Rankin, M., Stanton, P., McGowan, S., Ferlauto, K., Tiling, M., Meredith, K., & Antic, A. (2023). Theories in Accounting. In *Contemporary Issues in Accounting* (pp. 85-118). Milton Qld: John Wiley & Sons Australia Ltd.

Riaz, L., Hunjra, A. I., & Azam, R. I. (2012). Impact of psychological factors on investment decision making mediating by risk perception: A conceptual study. *Middle-East Journal of Scientific Research, 12(6)*, 789-795.

Rowe, B. R., & Gallaher, M. P. (2006). Private sector cyber security investment strategies: An empirical analysis. *The fifth workshop on the economics of information security (WEIS06).* England: Institute for Information Infrastructure Protection (I3P).

Safa, N. S., Solms, R. v., & Furnell, S. (2016). nformation security policy compliance model in organisations. *Computers & Security, 56*, 70-82.

Said, F., Abdul Jalil, A., & Zainal, D. (2023). Big Data Analytics Capabilities, Sustainability Reporting on Social Media, and Competitive Advantage: An Exploratory Study. *Asian Journal of Business and Accounting 16(1)*, 129-160.

Sekaran, U., & Bougie, R. (2016). *Research Methods for Business: A Skill-Building Approach. 7th Edition.* West Sussex: Wiley & Sons.

Sheikhpour, R., & Modiri, N. (2012). A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management. *Indian Journal of Science and Technology, 5(2)*, 2170-2176.

Simon, J., & Omar , A. (2020). Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *European Journal of Operational Research, 282(1)*, 161-171.

Suchman, M. C. (1995). Managing Legitimacy: Strategic and Institutional Approaches. *The Academy of Management Review, 20(3)*, 571-610 .

Sutherland, E. (2018). Cybersecurity: Governance of a New Technology. *Proceedings of the PSA18 Political Studies Association International Conference.* Cardiff: SSRN.

Taber, K. S. (2018). The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. *Research in Science Education, 48*, 1273–1296.

Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software engineering, 33(8)*, 544-557.

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk Management, 22*, 239-309.

Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security, 26(1)*, 2-9.

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.

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.