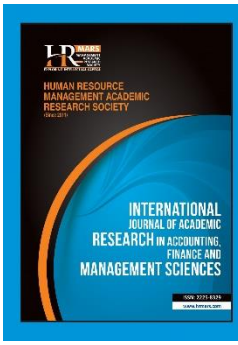


INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN ACCOUNTING, FINANCE AND MANAGEMENT SCIENCES

HRMARS MANAGEMENT ACADEMIC RESEARCH SOCIETY EXPLORING INTELLECTUAL CAPITAL

www.hrmars.com

ISSN: 2225-8329

Content Analysis of Voluntary Disclosures on Cybersecurity in Malaysia

Sharifah Norhafiza Syed Ibrahim, Adriana Shamsudin, Salina Abdullah, Mohd Tarmizi Ibrahim, Mohd Yassir Jaaffar and Hamidah Bani

To Link this Article: http://dx.doi.org/10.6007/IJARAFMS/v11-i4/11346 DOI:10.6007/IJARAFMS /v11-i4/11346

Received: *06* October 2021*, **Revised:** 14* November 2021*, **Accepted:** 29* November 2021

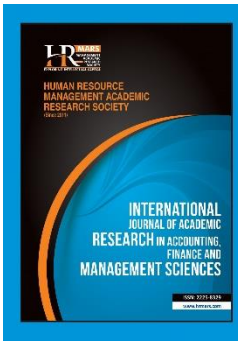
Published Online: 18 December 2021

In-Text Citation: (Ibrahim et al., 2021)

To Cite this Article: Ibrahim, S. 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.

Vol. 11, No. 4, 2021, Pg. 10 - 28

http://hrmars.com/index.php/pages/detail/IJARAFMS | **JOURNAL HOMEPAGE**


INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN ACCOUNTING, FINANCE AND MANAGEMENT SCIENCES
HRMARS MANAGEMENT ACADEMIC RESEARCH SOCIETY
EXPLORING INTELLECTUAL CAPITAL
www.hrmars.com
ISSN: 2225-8329

Content Analysis of Voluntary Disclosures on Cybersecurity in Malaysia

Sharifah Norhafiza Syed Ibrahim, Adriana Shamsudin, Salina Abdullah, Mohd Tarmizi Ibrahim, Mohd Yassir Jaaffar and Hamidah Bani

Universiti Teknologi MARA Melaka Malaysia

Abstract

Digitalisation is an important driver of the digital economy. The COVID-19 pandemic further accelerates the adoption of digital technology. Having huge data of clients, suppliers, investors, collaborators, and other business contacts expose companies to cyber threats and attacks. Several regulators such as the Security Exchange Commission (SEC) in the US requires public listed companies to disclose information related to cybersecurity risks. This study aims to explore how Malaysian listed companies reveal information related to cybersecurity in their annual reports. In addition, it also attempts to determine the themes or nature of these disclosures and to assess the disclosure levels. Using a content analysis, this study examined forty-nine annual reports from four sectors. It discovers that most companies disclose information related to cybersecurity under eight (8) common sections: governance and leadership, risk management and internal control, key risks and opportunities, management report, sustainability statement, organisational capital, external environment, and performance review. Furthermore, it suggests that these voluntary disclosures are mostly related to eight (8) themes: Data Protection Act, Data Security and Data Integrity, Cyber Threats and Risks, Cybersecurity Assessment, Focus and Priority, Optimisation, Enhanced and Investment, Policies and Artificial Intelligence. Even though most of these disclosures are at the basic level, there are a few companies with comprehensive disclosure on cybersecurity. The research findings provide valuable insights into voluntary disclosures related to cybersecurity among Malaysian listed companies.

Keywords: Voluntary Disclosures, Digitalisation, Cybersecurity, Sustainability

Introduction

Transforming businesses into digitalised business models is no longer an option to business entities as it is crucial for their current and future survivals. Digitalisation is an important driver of the digital economy. The COVID-19 pandemic further accelerates the adoption of digital technology. Commerce processes have become easier, faster, and scalable with electronic processing of orders, personal and banking information, and seamless access to information. Acknowledging its importance, the Malaysian government has launched the MyDigital initiative in the year 2021. This initiative reflects the country's long-term strategies

up to the year 2030 to reap the benefits of the digital economy, while safeguarding against its risks (Economic Planning Unit, 2021). One of the main challenges to successfully achieve the objectives of these strategies is cybersecurity. In the MyDigital initiative, the government highlights the importance of strengthening the cybersecurity ecosystem and ensuring that the public and businesses are aware of the importance of security in cyberspace.

Digitalisation of business models with its advances in information technology brings in unprecedented risks and threats of cybersecurity incidents to all companies (US Securities and Exchange Commission, 2018). Having huge data of clients, suppliers, investors, collaborators, and other business contacts may expose companies to cyber threats and attacks. Data fraud and cyber-attacks are among the top 10 risks to economic stability and social cohesion highlighted in the World Economic Forum (World Economic Forum, 2021). These risks could potentially disrupt business operations as well as the integrity of financial reporting. Thus, few regulators such as the Security Exchange Commission (SEC) require public listed companies to disclose cybersecurity risks. The SEC increased its scrutiny of public companies' disclosures of such hazards and their cybersecurity policies, processes, and controls to address cyber risks. Two most disclosed cybersecurity risks are risk of service or operation disruption and risks of data breach (Gao et al., 2020).

A clear and effective reporting to stakeholders, particularly the shareholders is one of five recommended proactive measures which demonstrate that the board of Malaysian companies are fulfilling their duties related to cybersecurity. These duties are to ensure that positions and actions on cybersecurity are well in place. The introduction of integrated reporting (IR) has changed the landscape of traditional financial reporting. Financial reports are no longer about past financial performance and position but more towards future oriented prediction and value creation. IR is expected to address some limitations of the financial statement, particularly being insufficient to reflect how values are created within the company. Upon the recommendation of the Securities Commission of Malaysia, Malaysian Institute of Accountant (MIA) established the Integrated Reporting Steering Committee in 2014. IR revolves around five key important areas which consist of materiality assessment, risk disclosure, consistency and comparability, internal and external factors impacting the business and the value creation business model. To consider global development in IR, Malaysia also collaborated with other ASEAN countries such as Singapore and Philippines. The collaboration was also to factor in the unprecedented pandemic COVID-19 that affected the way businesses were executed worldwide (Aucky Pratama, 2021). Many companies in Malaysia opt for integrated reporting despite it being non-mandatory.

Current business environment forces companies to integrate technology into their business models. Digital tools and technologies bring many benefits such as speed up business processes and boost productivity. However, companies face higher risks due to cyber threats. This will also put stakeholders' stake at greater risks. As part of investors' relation and communication, companies need to make voluntary disclosures related to cybersecurity. Users such as investors rely on descriptive information to gauge and analyse the future prospects of their investments. Unfortunately, not much is known about the nature and types of information relating to cybersecurity being disclosed in the annual reports. Annual reports could be a valuable source of descriptive information to users but not many studies investigate how they are providing necessary information to understand cybersecurity issues among Malaysian companies. This study aims to fill up this gap by exploring how Malaysian listed companies report information related to cybersecurity in their annual reports. In addition, it also attempts to determine the themes or nature of these disclosures and to

assess the disclosure levels. It shall provide insights into how Malaysian listed companies present information related to cybersecurity in their annual reports. Moving forward, digitalisation becomes the necessities for business entities. Hence, as part of demonstrating management's accountability to the stakeholders, cybersecurity should be voluntarily disclosed in the annual reports. This study contributes by providing recent evidence on what and how much have been disclosed by Malaysian companies. Such findings are useful to many users such as investors, financial analysts, financial institutions, suppliers of long-term funds, regulators, and Malaysian authorities.

Literature Review

Digitalisation and Cybersecurity

Fast development of Internet of Things or IoT has made major companies shift their main businesses into digitalisation through IoT. IoT can be defined as a system of interrelated computing devices with the ability to transfer data over a network without human-to-human or human-to-computer interaction (Gelenbe et al., 2018). It can be seen through the combination of traditional supply chain and IoT. This combination has led to the introduction of Cyber-physical system (CPS) to increase the efficiency of supply chain between organization and all interested parties such as supplier and the public (Humayed et al., 2017; Chandok & Singh, 2017; Kane et al., 2020). The rapid development of IoT also resulted in the development of new applications to capture, store, and protect data and the increase demand for a new level of protection for applications. However, the emergence of those applications also comes with threats (Brown, 2019). Companies nowadays need to focus more on securing their data due to increasing threat to cyber fraud and repercussions of the COVID-19 pandemic (Ma & McKinnon, 2021). This threat not only affects big companies but also Small and Medium Enterprise (SME). SMEs also has become constant targets of cyber-attacks Gerard Hoberg & Lewis (2017) which forced SMEs to shift their focus from improving systems to protecting businesses from cyber-attacks (Whitehead, 2020).

Protection against threats brought by the development of IoT is known as cybersecurity. The development of cybersecurity is not new (Healy & Palepu, 2001; Warner, 2012) and the increasing cases of frauds and threats has made it a main priority for companies (Gcaza et al., 2017). Cybersecurity can be defined as the protection and preservation of confidentiality, integrity, and availability (CIA) of information in the realm of cyberspace (IEC 27032/IEC 27032, 2012). Based on Warner (2012), there are three categories of threats towards cybersecurity namely human vulnerabilities, hardware vulnerabilities and software vulnerabilities. The protection of data has become more important than previous years and resulted in companies increasing their security over data from outside threats including internal threats (Ebert et al., 2019). Companies spending on cybersecurity measures also increase from time to time because of the increased cyber threats. Most companies believed that their spending on cybersecurity will keep increasing in the future (Kissoon, 2021).

Voluntary Disclosures

Embong (2014) defined corporate disclosure as a process of providing information to either internal or external users in making business decisions. Based on literature, corporate disclosure research focuses on either mandatory or voluntary disclosures (Bamber et al., 2010; Embong, 2014). Voluntary disclosures can frequently be seen in annual reports under sections of corporate features such as corporate size, board composition, listing status (Braam & Borghans, 2014; Bamber et al., 2010), strategic, financial, corporate social responsibility, and employee's information (Embong, 2014).

Voluntary disclosure may reduce information asymmetry and further lower a company's litigation risk as the more information being disclosed, the more credible, trustworthy, and persuasive the information (Healy & Palepu, 2001). Voluntary disclosure on digitalisation allows companies to make unique disclosures, which enable them to 'tell their own story' but at the expense of the comparability aspects (Shan & Troshani, 2021; Troshani et al., 2015). Shan & Troshani (2021) has found that by implementing digital corporate reporting technology among US firms will enhance value relevance. Lalević Filipović et al. (2018) explored information technology (IT) literacy of financial reporting in the local government of Montenegro and found that the use of websites is not mandatory, and the local government has very low transparency. Nurunnabi & Hossain (2012) examined the progress of voluntary disclosure on internet financial reporting in Bangladesh. With a sample of 285 listed companies, only 33.34% of companies disclosed voluntary information in the annual reports and these companies were all non-family owned and being audited by big audit firms. Based on Bamber et al. (2010), voluntary disclosures may enhance a company's ability to convey information on company performance and governance to external users. Oluwagbemiga (2014) also discovered that high levels of voluntary disclosure effectuate firms' higher performance as it provides investors with better information to make investment decisions. Burns et al. (2017) discovered that tone textual disclosures in the annual reports provide narrative disclosures that reduce information asymmetry. Therefore, they help investors to predict company performance for the next accounting period. Tran et al. (2021) provide further evidence that supports the effects of voluntary disclosures on the ability of financial statements to summarise firms' values.

However, looking from informational perspectives, voluntary disclosure can damage a company's competitive position (Bamber et al., 2010). Tran et al (2021) reveal that the narrative disclosures in the annual report reflect remarkable signals of company prospects in emerging markets, it will not be in favour the management. Lakshan et al. (2021) studied the future-oriented information that is required by the Integrated Reporting (IR) Framework and indicate that they may lead higher inherent risks related to uncertainties and predictions. They suggest several ways to overcome this such as making non-specific predictions, increasing the accuracy of estimation, ensuring specific employees achieve the agreed targets, reporting explanation on previous unachieved targets, and linking those predictions with company's risk management procedures. Furthermore, Shan & Troshani (2021) find that when digital corporate reporting technology is being implemented among Japanese firms, there is no difference in value relevance of reported information. Financial reports also have been questioned for its relevance to provide specifically on future-oriented information to the stakeholders (Lakshan et al., 2021).

Integrated Reporting

History of integrated reporting (IR) started in the early 2003 by a Denmark company. Since then, the demand for IR from users proves its impact on adding value to the existing financial report. IR is probably the future of the current financial statements. It is about communicating the strategy, governance, performance, and prospects that lead to the creation of value over the short, medium, and long-term. After 7 years, international IR committees were formed in England and Wales, which was participated by regulators, investors, companies, standard setters, the accounting profession, and NGOs worldwide. In December 2013, the first IR was published and until January 2021, the committees had gone through consultations with 1,470 individuals in 55 jurisdictions.

Rinaldi et al (2018) argue that IR is still at an early stage. Nevertheless, this area has been one of the growing research areas in accounting. Even though generally accepted and enforceable standards for IR are not yet available, companies are aware of its importance. They continue to incorporate IR in their report. Rinaldi et al (2018) suggest that IR can be divided into 5 journeys which are generation, elaboration, championing, production, and impact. Hameed & Rahman Ahmed (2020) indicate that from 2017 to 2019, small companies in Bahrain have moved towards preparing IR even though it is not yet mandatory. Furthermore, the study found out that larger companies tend to provide more comprehensive integrated reporting. IR is still on a voluntary basis too in Malaysia (Mohammed et al., 2020). Companies face many challenges to incorporate IR in the annual reports. Mohammed et al (2020) claim that there was a lack of understanding and lack of guidance on how to prepare the IR. However, many companies agreed that IR can improve their relationship with the stakeholder and suggested that IR must be made mandatory in Malaysia (Mohammed et al., 2020).

Cybersecurity Voluntary Disclosures

In the current context of the real business environment, millions of transactions are exercised across the globe without interference of physical market and tangible assets or services with the existence of digital technology embodied at the fingertips. There is a relevant loss to the existing accounting and reporting system if no significant changes are modified on the existing accounting practices to react to the current development of the digital economy. The new formation of financial reporting could increase the transparency of business and create a new dimension of business reporting to provide more insight by making reliable information on financial reports publicly available (Kulikova & Mukhametzyanov, 2019).

Current studies revealed that 87% of Dutch public listed companies disclosed cybersecurity related information in their annual reports even though there is no mandatory legal requirement to disclose such information. However, some of the strategic entities such as some Dutch banks and employment companies which are highly vulnerable to cybersecurity incidents did not disclose significant cybersecurity strategies and measures to overcome the operational risk and threats related to their nature of business (Eijkelenboom & Nieuwesteeg, 2021). This will give a negative signal to the shareholders and other stakeholders about the sustainability of the business prospect in the future especially the threat and risk of cybersecurity issues faced by the business. The transparent disclosures related to cybersecurity such as the capital investment acquired to overcome the threat and relevant strategy to face the cybersecurity issues are important to provide strong confidence on the prospect of future businesses.

Corporate governance plays a vital role to govern the entities. Complying with the relevant codes of corporate governance helps to ensure the sustainability of the business. The urgency of corporate governance practices among the publicly listed companies is to respond to the major corporate scandal in early 2000s. However, due to the current business environment, the business switch to the technological based entity, the information aspect of corporations including the cybersecurity governance, artificial intelligence governance and cloud governance need to be strengthened (Thuraisingham, 2020). Due to the exponential data administered by the entity, most of the corporations are migrating their data, software, and processes to cloud storage. Therefore, the entity needs to govern their cloud data by using appropriate policies and procedures integrated with its cyber strategies to avoid any risk associated with cybersecurity. The deployment of current technologies to mitigate the

cybersecurity risk could give a positive impact on the prospect of future business performance.

The voluntary disclosure of digitalisation-related information is considered an intellectual capital disclosure to investors to make relevant capital investment decisions. According to Ricci et al. (2020), the company with a good reputation on corporate responsibility (CR) strengthens the relationship between disclosure level of digitalisation with stock market valuation. Hence, the significant investment on digitalisation and proactive effort on corporate responsibility to society would increase firms' stock value and maximise the shareholders' wealth.

The significant effects of the digitalisation could catalyse the transition towards sustainable manufacturing practices among the multinational businesses. The smart and green technology embedded in the digitalisation platform could address the tremendous challenges of endangered climate change and planet biodiversity. Thus, it will contribute to the increase in humans' health wellbeing and towards building a sustainable society in the future (Mondejar et al., 2021). Based on a study conducted by Del Río Castro et al. (2021), there is a positive outlook on added value brought by the digitalisation of future business sustainability through digital ecosystem and environment. According to D'amico et al. (2021), the digitalisation initiatives implemented by the municipalities of Kaunas, Flanders region, Proto, The Hague, and Oslo in the European Union intended to increase the efficiency of the circularity of urban metabolic flows. The digitalisation practices involved the monitoring stations for water and energy consumption, installing digital cameras for traffic flows, disseminating information through web-based platforms and setting up tracking sensors for public transport.

Malaysian listed companies voluntarily disclosed some information related to their journeys in adopting digital tools and technologies (Zeranski & Sancak, 2020; Ibrahim et al., 2021). They basically describe their digitalisation initiatives in the year 2020 and their plans and strategies related to transforming their businesses into digital business models. Therefore, it is also important for companies to inform their stakeholders about their cybersecurity matters. This study attempts to investigate how Malaysian companies voluntarily disclose information about how they address cybersecurity in the annual reports.

Research Methodology and Methods

This paper used a qualitative approach where it analysed data from the annual reports. As it was designed to assess how Malaysian listed companies voluntarily disclosed information related to cybersecurity in the annual reports, content analysis was used to gather the required data. The study population was all listed companies on the Bursa Malaysia. Four sectors were selected based on the four sectors that were most likely to be affected by cybersecurity. These sectors were technology, media and telecommunications, consumer products and services, and energy.

A purposive sampling technique was utilised where companies that met three predefined conditions were selected. First, the 2020's audited published annual reports were made available at their website and second, the word 'cybersecurity' was disclosed somewhere in the annual reports. Third, a company was from one of the four sectors.

There were forty-nine (49) companies that met the required conditions and hence, they were selected as the study sample. The number of companies was nineteen (19) from consumer products and services, seven (7) from energy, ten (10) from technology and thirteen (13) from media and telecommunications sectors. The annual reports for the year

2020 were downloaded and then analysed using ATLAS.ti 8 in order to achieve the research objectives.

Four researchers were assigned with the data collection task. Each researcher was responsible to collect the annual reports and code the data using the ATLAS.ti 8 for one sector. A standardised codebook designed by the principal researcher was utilised. The coding was developed based on a pilot study from a smaller sample. ATLAS.ti 8 was used to organise and analyse the documents. The analysis and coding focused on three areas related to the research questions: disclosure sections, the themes or nature of the disclosures, and the assessment of the disclosures.

Discussion of Results and Findings

This section presents and discusses results related to the research objectives. The first research objective was to explore how Malaysian companies disclosed information related to cybersecurity in their annual reports. The second objective was to examine the themes or nature of these disclosures and the third objective was to assess the disclosure levels.

Preferred Sections for Cybersecurity-related Disclosures

Figure 1 and Table 1 presents results related to the first objective. Figure 1 shows eight common sections companies used to present information related to cybersecurity. These sections were labelled as sustainability statement, governance and leadership, key risks and opportunities, external environment, management report, risk management and internal control statement, organisational capital, and performance review.

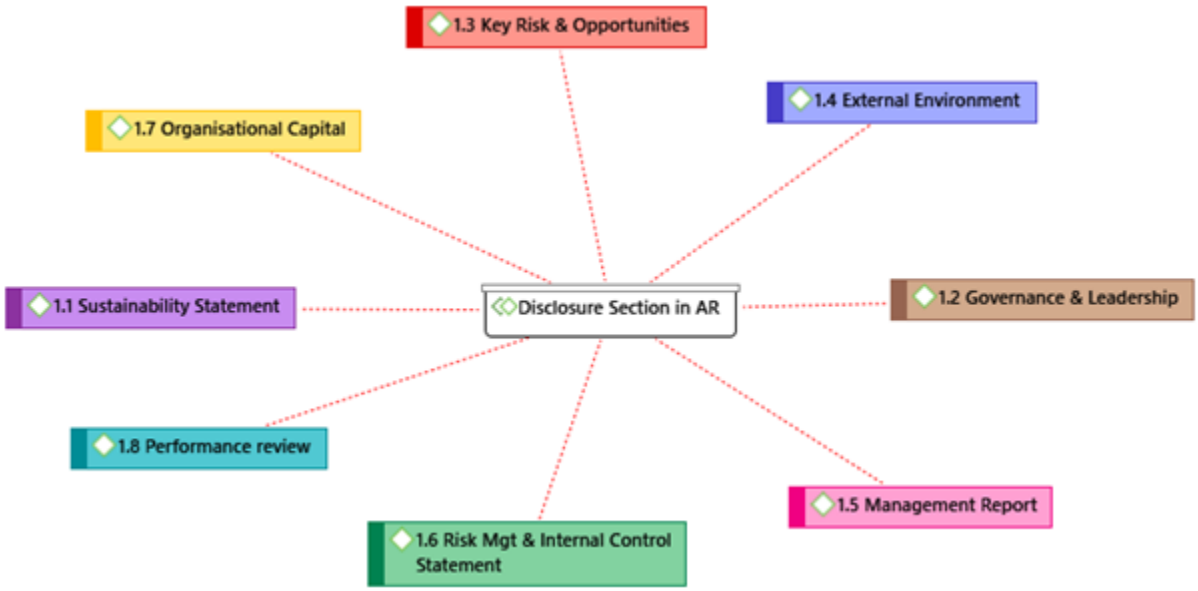


Figure 1: Preferred Sections for Reporting Cybersecurity in the Annual Report

Table 1 shows the frequency of disclosures related to cybersecurity by Malaysian companies for each of the eight sections across the four sectors. The most common section based on frequency was governance and leadership. Reviewing and monitoring risks including cybersecurity risks are part of board of directors' responsibilities (Thuraisingham, 2020). This might explain why many companies' disclosures related to cybersecurity were included in the governance and leadership section. The second most preferred section was risk management and internal control.

Table 1: Preferred Sections for Reporting Cybersecurity in the Annual Report (frequency)

	Consumer Products & Services	Energy	Technology	Media & Telecom.	TOTAL
Sustainability Statement	6	5	8	8	27
Governance and Leadership	13	10	7	24	54
Key Risk and Opportunities	6	1	9	14	30
External Environment	nil	1	2	nil	3
Management Report	6	nil	19	4	29
Risk Mgt. and Internal Control Statement	25	3	nil	16	44
Organisational Capital	nil	7	nil	2	9
Performance review	2	1	nil	nil	3
TOTAL	**58**	**28**	**45**	**68**	**199**

The third section that companies used to provide information related to cybersecurity is the section on key risks and opportunities. Digitalisation brings greater opportunities. However, it also increases companies' cybersecurity vulnerabilities. Companies disclosed their approach in cybersecurity risk management, including identification of cyber threat as risk drivers and key business scenarios. The next highly used section is a management report. Acting as an agent, management is responsible to ensure the principal's investment is well-managed and safeguarded. Reporting on how and what management has done to monitor and minimise cyber threats may enable companies to 'tell their own story' Shan & Troshani (2021) in dealing with cybersecurity. Maintaining clients' trust and loyalty is crucial for a company's survival. Hence, disclosures related to cybersecurity is also reported in the sustainability statement. Doing business today means ensuring a client's peace of mind through data security and privacy is essential for the business consideration. In the sustainability statement, many companies disclosed that their employees' skills and knowledge in handling cybersecurity issues were continuously updated. The other three sections that this study found were organisational capital, external environment, and performance review. However, these three sections were not being used by majority companies to disclose information related to cybersecurity.

Table 2: Preferred Sections for Reporting Cybersecurity in the Annual Report (percentage)

	Consumer Products & Services	Energy	Technology	Media & Telecom.	TOTAL
Sustainability Statement	10%	18%	18%	12%	14%
Governance and Leadership	22%	36%	16%	35%	27%
Key Risk and Opportunities	10%	4%	20%	21%	15%
External Environment	nil	4%	4%	nil	2%
Management Report	10%	nil	42%	6%	15%
Risk Mgt. and Internal Control Statement	43%	11%	nil	24%	22%
Organisational Capital	nil%	25%	nil	3%	5%
Performance review	3%	4%	nil	nil	2%
TOTAL	**100%**	**100%**	**100%**	**100%**	**100%**

Table 2 illustrates the popularity of the eight sections commonly used by Malaysian listed companies in percentage. Hence, the same discussion of results related to Table 1 applies here. For example, 27% of information related to cybersecurity were reported in governance and leadership section. It was the most used section for energy and media and telecommunication sectors. The second most used section is the risk management and internal control statement which reflected 22% of the total observations/counts. However, this section was the most used section for companies from consumer products and services sector.

The Themes or Nature of Cybersecurity-related Disclosures

The annual report from four different industries has been analysed and scrutinised for their disclosures on cybersecurity to identify common themes of the disclosures. Based on our pilot analysis, the themes can be divided into eight (8) themes which are Data Protection Act, Data Security and Data Integrity, Cyber Threats and Risks, Cybersecurity Assessment, Focus and Priority, Optimisation and Enhanced Investment, Policies and Artificial Intelligence.

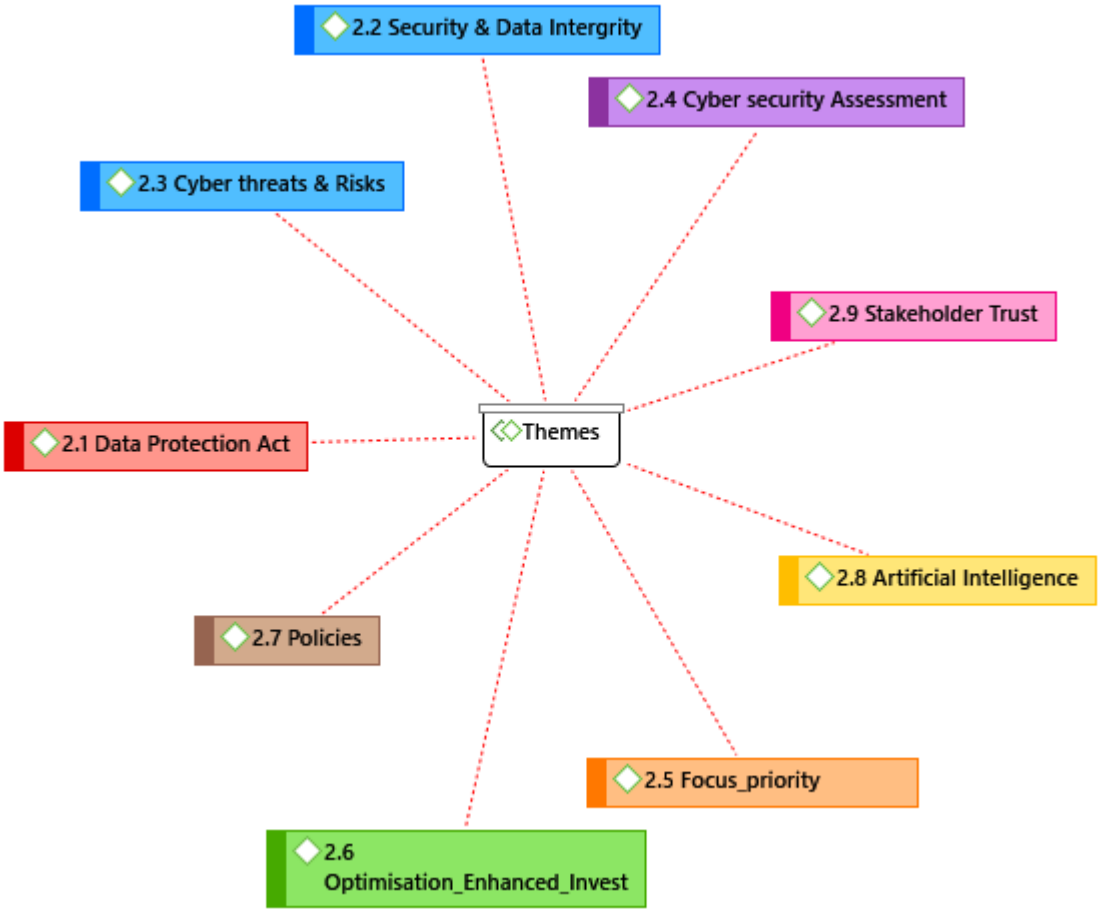


Figure 2: The Themes for Cybersecurity Related Disclosures

Table 3 shows the percentage for each theme across the four sectors. The following paragraphs further discuss our findings based on the total percentage for each theme. Most of the cybersecurity-related disclosures pertained to cyber threats and risks. The next most common theme was security and data integrity, policies, and cybersecurity assessment.

Table 3: The Themes for Cybersecurity-related Disclosures (percentage)

	Consumer Products & Services	Energy	Technology	Media & Telecom.	TOTAL
Data Protection Act	3%	24%	7%	20%	6%
Security & Data Integrity	13%	24%	nil	20%	16%
Cyber Threats & Risks	34%	24%	17%	24%	25%
Cybersecurity Assessment	13%	9%	26%	14%	15%
Focus/Priority	13%	9%	15%	14%	13%
Optimise Investment	11%	12%	9%	3%	7%
Policies	11%	6%	24%	17%	16%
Artificial Intelligence	nil	6%	2%	1%	1%
TOTAL	**100%**	**100%**	**100%**	**100%**	**100%**

Cyber Threats, Risks and Cybersecurity Assessment

Table 3 shows that 25% and 15% of cybersecurity disclosures is related to cyber threats and risks and cybersecurity assessment respectively. Therefore, these themes are the most common themes for disclosures on cybersecurity, representing 40% of the whole disclosure counts. Rapid advancement in technology has shifted the cyber threats landscape all over the world. It must not be seen as insignificant because the company must ensure the business continuity will not be affected by cyber threats. In addition, the company must always protect the workers and its customers from any unnecessary risk in the cyber world. As companies move towards digitalisation, companies are also exposed to greater cybersecurity risk. Companies disclosed that most of the major threats of cybersecurity risk are ransomware, phishing, hacking, data leakage including data damages and internal threats. Companies recognize cyber threats and include the risk as one of their major business risks to be continuously reviewed to secure their IT system.

Based on the disclosures on cybersecurity, most of the companies recognise the cybersecurity threats and risk by implementing IT Security Policy, Cybersecurity Framework, End User Policy and Access Management based on the ISO 27001 certificate. The policy and framework introduced by the companies aim to secure the companies' information system and increase customer confidence in participating in online activities with the companies. Companies also provide training and create awareness among their staff to build a strong IT security culture. Additional safety measures such as security logging monitoring programs to monitor all network activities by staff to detect any anomalies are also being implemented to increase the safety of the company's IT system. This also ensures only staff that has access to related sections has the access and avoid any data breach.

Companies also set up a cybersecurity team for detecting potential cyber-attack, mitigating and continuously conducting security assessment to ensure their IT systems are resilient towards cyber threats. The team is responsible for making sure that companies' IT

systems are secured from cyber-attack when staff are working from home in the era of digitalisation and COVID-19 as well as protecting customer data. Protecting company's data from cyber theft, data corruption and customer data has been recognized as top priority by the management. To ensure the safety of the data, companies continuously review their IT Systems by implementing the latest Antivirus Systems and Firewall systems from their Cybersecurity team recommendations.

Data Protection Act & Security and Data Integrity

In comparison to other business themes, Data Protection Act and Security and Data integrity represent 6% and 16% of the total counts of disclosures-related to cybersecurity respectively. Digitalisation causes companies to give heed to security challenges. When companies adopt digitalisation in their marketing, business processes, products, and many other aspects of businesses, they must assure stakeholders that they do consider data protection and technological advances to secure the digitalisation initiatives. Voluntary disclosures on cybersecurity are a practical way to communicate this to stakeholders, particularly the investors. Some companies reported that cybersecurity is strictly important as it is governed under Malaysian Personal Data Protection Act 2010 ("PDPA") which requires protection of data privacy for customers, employees, and business partners. Companies disclose that they align cybersecurity initiatives with other guidelines and standards like NIST1 Framework, AICPA/CICA2 and CMMI3 Privacy Maturity models. There are companies who established systems like Information Security Management System ("ISMS") ISO/IEC 27001:2013[1], Payment Card Industry Data Security Standard v3.2.1 and continuously benchmark their security programme based on industry's best practices. This acts as important and relevant safeguards with latest security control to overcome any emergence of cyberattacks and threats. Some companies had established new company policies such as Group Data Privacy Policy, "Digital Trust 2020" into "Digital Trust and Resilience – DT&R2023" and created new privacy teams to enhance cybersecurity controls like Cybersecurity Advisory.

When we analysed data security and data integrity disclosures in annual reports, we discovered some companies had set up special teams or committees to specifically monitor and supervise data security management practices. However, we also found that there were some companies that engaged with external consultants to conduct assessments of their systems and to react to any cyberattacks and threats. Most companies intensified their ability to identify, prevent, detect, and respond to data security threats in a prompt period by conducting tests and simulation. In addition, they assessed systems' capabilities to overcome any cybersecurity risk like real-time threat monitoring, alert analysis and response, crisis simulation testing, crisis simulation game on cyberhacking, vendor risk assessment, Message Blast Test, and Call Tree Test.

Apart from conducting rigorous assessment tests to check the vulnerability of the system security, most companies acted proactively by sending their employer to privacy awareness training such as supplier's privacy training, mandatory cybersecurity awareness training, scenario-based learning on phishing, mobile security and everyday security training as well as performing simulations to assess employees' resilience knowledge and general awareness. Besides, companies designed alternative drives to elevate data security and integrity such as protecting hardware and software, reducing third party risk through Supplier Code of Conduct, securing customer's data confidentiality, performing security audits, setting up protection on data privacy breaches, firewall and perimeter security, placing control on active virus and safeguarding confidential information from external hackers.

Focus/Priority

Next, we observed the other two common themes were focus and priority (13%) and policies (16%). Companies disclosed that cybersecurity continued to be a strong focus in 2020. They implemented several initiatives to minimise key risks which includes operational, technological and cybersecurity related risks. Special budgets were allocated to invest in the latest technology and infrastructure to ensure business and operations were adequately supported. Companies were also consistently improving their network security to minimise the threats of cyber-attacks, data theft and information leakage. Employee training related to digital security was also one of the focused areas. Companies provided information about cybersecurity awareness workshops such as those conducted by technology companies. Their IT experts facilitated the complimentary workshop to drill participants to raise awareness among clients and partners on cybersecurity. These workshops provided many benefits. For example, enhanced employees' and vendors' cybersecurity and privacy awareness, knowledge, and skills, ensured strong alignment with global best practices, and strict regulatory compliance in data privacy. Group-wide Cybersecurity and Privacy training and awareness programme enhanced employees' and vendors' knowledge and capabilities through updated modules covering data privacy, current digital risks, and cyber threats.

Optimisation and Enhanced Investment and Policies

In addition, based on our analysis of the disclosures, companies explained that investment in the latest technology was paramount to ensure that the growing customer base was continuously met and remains well served. Optimisation and enhancement of investment was another theme for the disclosures from companies (7%). Initiatives launched by the Malaysian government such as JENDELA, which aims to accelerate digital connectivity through widespread deployment of fibre and mobile whilst exploring other fit-for-purpose technologies such as fixed wireless access (FWA) further justified and accelerated the investment in related infrastructure.

Our analysis also found that most of the companies set up a team led by a Risk Manager within the IT Department that will focus on the cyber threats. The team will continuously review the company's cyber framework and make recommendations to the management to update their hardware or software to ensure their system is safe from cyber-attack. This cyber framework will serve as the company's policy in safeguarding their system. The analysis also found that most of the investments made by the companies in upgrading or ensuring their system are focusing on data privacy and avoiding data leakage. The team is also responsible to provide training to the staff relating to the company's system. Apart for that, most of the companies also ensure they will keep updating and investing in reliable hardware or software including installation of latest Antivirus programmes and Firewall. Companies pledge to continuously update their system in response to changes of customer and staff work-life behaviours. The COVID-19 pandemic has made staff work from home which force companies to maintain a safe and reliable system. Apart from that, by having a sound online system that enables staff to work from home and avoid any interruption on daily business activities with their supplier and customers. Companies also need to maintain the latest technology and safe system due to customer behaviour that has changed from the traditional method of buying by going to shop to buying online using their devices such as mobile phones and through company websites. Companies recognised the importance of updating their system and investing in the latest technology were essential to make sure they survived in the era of digitalisation and the COVID-19 pandemic.

Artificial Intelligence

The last theme was artificial intelligence. It can be defined as simulation of human intelligence processes by machines, especially computer systems (Burns et al., 2017). However, the disclosure on artificial intelligence is not much being disclosed in the annual report. Most companies did not disclose about artificial intelligence. Out of forty-nine companies that have been scrutinised, only four of them have disclosure on artificial intelligence. Basically, the disclosure stated that the company developed strategies to reinvent cybersecurity escorted with artificial intelligence (AI). The companies only mentioned in brief about artificial intelligence that has been implemented in the company in one sentence only and no further elaboration has been discussed on the implementation. This may indicate that AI have not yet morphed as one of Malaysia's business models.

Cybersecurity-related Disclosure Levels

The third objective intends to assess how much information related to cybersecurity is disclosed by Malaysian listed companies. This study used three levels of disclosures: basic, adequate, and comprehensive. Table 4 and 5 present the results.

Table 4: Assessment of Disclosure Levels (counts) Related to Cybersecurity

	Consumer Products & Services	Energy	Technology	Media & Telecom.	TOTAL
Basic	45	5	38	51	139
Adequate	9	17	7	15	48
Comprehensive	nil	nil	nil	3	3
TOTAL	**54**	**22**	**45**	**69**	**190**

Overall, this study finds most Malaysian companies disclose general and brief descriptions and explanation of cybersecurity. Table 4 shows that 139 occurrences of basic disclosures on cybersecurity or 73% (Table 5) of the total disclosures is at the basic level. However, these results indicate some disclosures contain specific information related to cybersecurity initiatives, plans and measures undertaken by companies. Such disclosures are assessed to be at the adequate level. There were 48 adequate disclosures, representing 25% of total disclosures on cybersecurity. Media and telecommunication companies co-exist with digital tools and technologies. Therefore, cybersecurity is an important matter to address by the companies. It is not surprising to see few of them provided comprehensive disclosures on cybersecurity. Those disclosures were very focused and dedicated specific section for disclosing information related to cybersecurity. Not only their disclosures were specific but also supported by financial information such as projected impact on efficiency, productivity, incurred costs and other financial implications of the cybersecurity initiatives and measures.

Table 5: Assessment of Disclosure Levels (percentage) Related to Cybersecurity

	Consumer Products & Services	Energy	Technology	Media & Telecommunications	TOTAL
Basic	83%	23%	84%	74%	73%
Adequate	17%	77%	16%	22%	25%
Comprehensive	nil	nil	nil	4%	2%
TOTAL	**100%**	**100%**	**100%**	**100%**	**100%**

Conclusion, Limitations and Future Research

Current business environment forces companies to integrate technology into their business models. Digital tools and technologies bring many benefits such as speed up business processes and boost productivity. However, companies face higher risks due to cyber threats. This will also put stakeholders' stake at higher risks. As part of investors' communication, companies need to make voluntary disclosures related to cybersecurity. This study explores how Malaysian companies disclosed information related to cybersecurity in their annual reports, the themes or nature of these disclosures and the disclosure levels. This paper only focused on 4 sectors: consumer products and services, energy, technology and media and telecommunication. Content analysis was the main method for both data collection and analyses.

This study suggests that most companies disclose information related to cybersecurity under eight sections of the annual report. These sections by ranking are governance and leadership, risk management and internal control, key risks and opportunities, management report, sustainability statement, organisational capital, external environment, and performance review. Next, this study finds these voluntary disclosures are mostly related to eight (8) themes: Data Protection Act, Data Security and Data Integrity, Cyber Threats and Risks, Cybersecurity Assessment, Focus and Priority, Optimisation, Enhanced and Investment, Policies and Artificial Intelligence. In addition, most of the disclosures is at the basic level. About a quarter of the disclosures is at adequate level. Nevertheless, there are few companies with comprehensive disclosures on cybersecurity.

Companies are required to publish annual reports. Over the years, the annual reports have evolved where companies not only furnish mandatory information but also voluntary disclosures. This study contributes by providing new evidence of voluntary disclosures. It specifically offers insights into how companies disclose information related to cybersecurity, the common themes of such disclosures and how much this information is being disclosed in the annual reports. The study findings are relevant to both the preparers and users of annual reports. They can be useful indicators to preparers that disclosures related to cybersecurity are increasing and are of interests to users. This is important as technologies are embedded and integrated into the business models which expose companies to cyber threats and attacks. For users, particularly investors, disclosure on cybersecurity might be useful to them and helps investors to get bigger picture of the stability and sustainability of their investments. They may be assured by having such disclosures available in which companies describe, explain, and justify measures and initiatives to mitigate cyber risks. Other than

providers and receivers of disclosures on cybersecurity, the study findings may also be significant to regulators. The study provides regulators recent evidence on voluntary disclosures in general and disclosures on cybersecurity that can help regulators to assess current trends in voluntary disclosures and predict its future directions. Malaysia strives to keep the nation up to date with the technological advancement and implements various initiatives to facilitate business players in integrating technologies into their business models. Cybersecurity is acknowledged as the main obstacle in becoming a digitalised nation. Therefore, this study provides useful evidence related to how Malaysian public listed companies address cybersecurity. Such evidence may be relevant for the Malaysian authorities in evaluating the effectiveness of their initiatives related to cybersecurity. It can also be used as useful inputs in formulating future strategies that can help Malaysia to realise its aspiration to become a thriving digitalised nation.

This study findings are limited by several factors such as it covers only four sectors in Malaysia and the variations in coding the disclosures by researchers. Future research can include more sectors and use better instruments in analysing the data.

Acknowledgment

The research was supported by Universiti Teknologi MARA Melaka Branch through the Teja Internal Grant 2021 (GDT2021/1-11).

References

Pratama, A. (2021). Integrated Reporting in ASEAN | Accountants Today. *Mia*, 1–5. https://www.at-mia.my/2021/05/27/integrated-reporting-in-asean/

Bamber, L. S., Jiang, J., & Wang, I. Y. (2010). What's my style? The influence of top managers on voluntary corporate financial disclosure. *Accounting Review*, *85*(4), 1131–1162. https://doi.org/10.2308/accr.2010.85.4.1131

Braam, G., & Borghans, L. (2014). Board and auditor interlocks and voluntary disclosure in annual reports. *Journal of Financial Reporting and Accounting*, *12*(2), 135–160. https://doi.org/10.1108/jfra-11-2012-0054

Burns, E., Laskowski, N., & Tucci, L. (2017). *What is artificial intelligence?* TechTarget. https://searchenterpriseai.techtarget.com/definition/AI-Artificial-Intelligence#:~:text=Artificial intelligence is the simulation,speech recognition and machine vision.

Chandok, R. I. S., & Singh, S. (2017). Empirical study on determinants of environmental disclosure: Approach of selected conglomerates. *Managerial Auditing Journal*, *32*(4–5), 332–355. https://doi.org/10.1108/MAJ-03-2016-1344

D'amico, G., Arbolino, R., Shi, L., Yigitcanlar, T., & Ioppolo, G. (2021). Digital technologies for urban metabolism efficiency: Lessons from urban agenda partnership on circular economy. *Sustainability (Switzerland)*, *13*(11), 1–23. https://doi.org/10.3390/su13116043

Del Río Castro, G., González Fernández, M. C., & Uruburu Colsa, Á. (2021). Unleashing the convergence amid digitalization and sustainability towards pursuing the Sustainable Development Goals (SDGs): A holistic review. *Journal of Cleaner Production*, *280*. https://doi.org/10.1016/j.jclepro.2020.122204

Ebert, M., Schäfer, U., & Schneider, G. T. (2019). Information Leaks and Voluntary Disclosure. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3372141

Economic Planning Unit, P. M. D. (2021). *Malaysia Digital Economy Blueprint.* Malaysian

National Library. https://www.epu.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf.

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

Embong, Z. (2014). Understanding Voluntary Disclosure: Malaysian Perspective. *Asian Journal of Accounting and Governance*, *5*, 15–35. https://doi.org/10.17576/ajag-2014-5-02

Gao, L., G.Calderon, T., & FengchunTang. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, *38*.

Gcaza, N., Von Solms, R., Grobler, M. M., & Van Vuuren, J. J. (2017). A general morphological analysis: Delineating a cyber-security culture. *Information and Computer Security*, *25*(3), 259–278. https://doi.org/10.1108/ICS-12-2015-0046

Gelenbe, E., Domanska, J., Czáchorski, T., Drosou, A., & Tzovaras, D. (2018). Security for Internet of Things: The SerIoT Project. *2018 International Symposium on Networks, Computers and Communications, ISNCC 2018*. https://doi.org/10.1109/ISNCC.2018.8531004

Hoberg, G., & Lewis, C. (2017). Do fraudulent firms produce abnormal disclosure? *Journal of Corporate Finance*, *43*(C), 58–85.

Hameed, S. M. A., & Rahman Ahmed, N. A. R. (2020). Adoption of integrated reporting in emerging economies: Evidence from bahrain. *Asian Economic and Financial Review*, *10*(10), 1115–1130. https://doi.org/10.18488/journal.aefr.2020.1010.1115.1130

Healy, P. M., & Palepu, K. G. (2001). Information asymmetry, corporate disclosure, and the capital markets: A review of the empirical disclosure literature. *Journal of Accounting and Economics*, *31*, 405–440.

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-Physical Systems Security - A Survey. *IEEE Internet of Things Journal*, *4*(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172

Kane, G. A., Lopes, G., Saunders, J. L., Mathis, A., & Mathis, M. W. (2020). Real-time, low-latency closed-loop feedback using markerless posture tracking. *ELife*, *9*, 1–29. https://doi.org/10.7554/ELIFE.61909

Kulikova, L. I., & Mukhametzyanov, R. Z. (2019). Formation of financial reporting in the conditions of digital economy. *Journal of Environmental Treatment Techniques*, *7*(Special Issue), 1125–1129.

Lakshan, A. M. I., Low, M., & de Villiers, C. (2021). Management of risks associated with the disclosure of future-oriented information in integrated reports. *Sustainability Accounting, Management and Policy Journal*, *12*(2), 241–266. https://doi.org/10.1108/SAMPJ-03-2019-0114

Ma, K. W. F., & McKinnon, T. (2021). COVID-19 and cyber fraud: emerging threats during the pandemic. *Journal of Financial Crime*, *October*. https://doi.org/10.1108/JFC-01-2021-0016

Mohammed, N. F., Kassim, C. F. C., Sutainim, N. A., & Amirrudin, M. S. (2020). Accountability through integrated reporting: The awareness and challenges in Malaysia. *Humanities and Social Sciences Letters*, *8*(1), 123–132. https://doi.org/10.18488/journal.73.2020.81.123.132

Mondejar, M. E., Avtar, R., Diaz, H. L. B., Dubey, R. K., Esteban, J., Gómez-Morales, A., Hallam, B., Mbungu, N. T., Okolo, C. C., Prasad, K. A., She, Q., & Garcia-Segura, S. (2021). Digitalization to achieve sustainable development goals: Steps towards a Smart Green Planet. *Science of the Total Environment*, *794*(June), 148539. https://doi.org/10.1016/j.scitotenv.2021.148539

Nurunnabi, M., & Hossain, M. A. (2012). The voluntary disclosure of internet financial reporting (IFR) in an emerging economy: A case of digital Bangladesh. *Journal of Asia Business Studies*, *6*(1), 17–42. https://doi.org/10.1108/15587891211190688

Oluwagbemiga, O. E. (2014). The use of voluntary disclosure in determining the quality of financial statements: Evidence from the Nigeria listed companies. *Serbian Journal of Management*, *9*(2), 263–280. https://doi.org/10.5937/sjm9-5784

Ricci, F., Scafarto, V., Ferri, S., & Tron, A. (2020). Value relevance of digitalization: The moderating role of corporate sustainability. An empirical study of Italian listed companies. *Journal of Cleaner Production*, *276*, 123282. https://doi.org/10.1016/j.jclepro.2020.123282

Rinaldi, L., Unerman, J., & de Villiers, C. (2018). Evaluating the integrated reporting journey: insights, gaps and agendas for future research. *Accounting, Auditing and Accountability Journal*, *31*(5), 1294–1318. https://doi.org/10.1108/AAAJ-04-2018-3446

Shan, Y. G., & Troshani, I. (2021). Digital corporate reporting and value relevance: evidence from the US and Japan. *International Journal of Managerial Finance*, *17*(2), 256–281. https://doi.org/10.1108/IJMF-01-2020-0018

Ibrahim, S. N., Shamsudin, A., Ibrahim, M. T., Abdullah, S., Jaaffar, M. Y., & Bani, H. (2021). An Initial Assessment of Voluntary Disclosures on Digitalisation by Malaysian Public Listed Companies. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, *11*(3), 303–314. https://doi.org/10.6007/ijarafms/v11-i3/10966

Tara Kissoon, S. (2021). Optimum Spending on Cybersecurity Measures: Part II. *Journal of Information Security*, *12*(01), 137–161. https://doi.org/10.4236/jis.2021.121007

Thuraisingham, B. (2020). Cloud Governance. *2020 IEEE 13th International Conference on Cloud Computing (CLOUD)*.

Tran, L. T. H., Tu, T. T. K., Nguyen, T. T. H., Nguyen, H. T. L., & Vo, X. V. (2021). Annual report narrative disclosures, information asymmetry and future firm performance: evidence from Vietnam. *International Journal of Emerging Markets*, *502*. https://doi.org/10.1108/IJOEM-08-2020-0925

Troshani, I., Parker, L. D., & Lymer, A. (2015). Institutionalising XBRL for financial reporting: resorting to regulation. *Accounting and Business Research*, *45*(2). https://doi.org/https://doi.org/10.1080/00014788.2014.980772

US Securities and Exchange Commission. (2018). *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*. https://www.sec.gov/rules/interp/2018/33-10459.pdf

Warner, M. (2012). A Pre-history. *Intelligence and National Security*, *27*(5), 781–799. https://doi.org/10.1080/02684527.2012.708530

Whitehead, G. (2020). *Investigation of factors influencing cybersecurity decision making in Irish SME's from a senior manager/owner perspective*. *August*.

World Economic Forum. (2021). The Global Risks Report 2021: 16th Edition. In *Weforum.Org*. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

Zeranski, S., & Sancak, I. E. (2020). Digitalisation of Financial Supervision with Supervisory Technology (SupTech). *SSRN Electronic Journal*, *July*. https://doi.org/10.2139/ssrn.3632053