South African Journal of Economic and Management Sciences
ISSN: (Online) 2222-3436, (Print) 1015-8812

Exploring cybersecurity disclosure in South Africa

Authors:
Laura F. Putter[1]
Ruth Johnson[1]
Nadia Mans-Kemp[1]

Affiliations:
[1]Department of Business Management, Faculty of Economic and Management Sciences, Stellenbosch University, Stellenbosch, South Africa

Corresponding author:
Ruth Johnson,
rsolomons@sun.ac.za

Dates:
Received: 18 Feb. 2025
Accepted: 31 Oct. 2025
Published: 12 Jan. 2026

How to cite this article:
Putter, L.F., Johnson, R. & Mans-Kemp, N., 2026, 'Exploring cybersecurity disclosure in South Africa', *South African Journal of Economic and Management Sciences* 29(1), a6133. https://doi.org/10.4102/sajems.v29i1.6133

Background: The coronavirus disease 2019 (COVID-19) pandemic resulted in the increased use of technology by companies. As such, corporate leaders started giving due attention to escalating cybersecurity concerns and disclosing such information to stakeholders in integrated reports to enhance legitimacy.

Aim: The authors investigated cybersecurity disclosures by selected South African companies that were most vulnerable to cyber threats before and during the COVID-19 pandemic.

Setting: Disclosures by selected Banking, Health care, Technology and Retail companies that were listed on the Johannesburg Stock Exchange (JSE) were analysed between 2017 and 2022.

Method: Content analysis was conducted on integrated reports. Three cybersecurity disclosure metrics were computed, namely disclosure presence (the number of keyword occurrences), disclosure level (coverage scores based on the unique keywords used relative to the total number of keywords) and disclosure volume (number of paragraphs comprising cybersecurity information). Significant differences for the three disclosure metrics were assessed for the overall period and between the considered years by conducting sequential analysis of variance (ANOVA) and Fisher's least significant difference (LSD) analyses, respectively.

Results: The disclosure presence, level and volume of cybersecurity by sampled companies improved noticeably. Statistically significant differences were observed for the overall period for all three disclosure metrics. Most of the annual differences for cybersecurity disclosures were significant.

Conclusion: The sampled companies rapidly adopted and adapted their cyber-related practices and disclosures since 2020. The companies disclosed on key cybersecurity threats and the management thereof in their integrated reports to enhance their legitimacy.

Contribution: This study shows which cybersecurity matters received the most attention by the sampled JSE-listed companies in their integrated reports.

Keywords: cybersecurity; disclosure presence; disclosure level; disclosure volume; content analysis.

Introduction

Although companies globally and in South Africa are increasingly reaping the benefits associated with cybertechnology, numerous financial losses and reputational damages because of cybercrime were also reported (PricewaterhouseCoopers [PwC] 2022). Companies require appropriate cybersecurity frameworks and systems to withstand such attacks (Eling & Schnell 2016). Since the advent of the coronavirus disease 2019 (COVID-19) pandemic, cyber risks, threats and attacks, and by implication the need for enhanced cybersecurity, have become even more prevalent (Accenture 2021a).

Cybersecurity refers to technologies, processes and organisational structures that protect a company's information technology (IT) networks and systems from security flaws, breaches and infringements on intellectual property rights (Craigen, Diakun-Thibault & Purse 2014). Cybersecurity structures and systems thus guard companies against various types of potential cyber risks, threats and attacks (Zwilling 2022).

The World Economic Forum (2022) confirmed that cyber risks challenge corporate leaders globally. As such, risk management is an essential corporate governance matter to ensure that

cybersecurity concerns are sufficiently addressed. Yet several corporate leaders view cybersecurity as an IT consideration rather than a pertinent corporate governance issue (Clinton 2022).

In light of the substantial increase in cybercrime, researchers, shareholders and regulators are increasingly expecting companies to disclose information on cybersecurity matters (Bravo 2017; Institute of Directors in South Africa [IoDSA] 2016; Radu & Smaili 2021). To enhance their legitimacy, companies attempt to disclose sufficient details on material matters, such as their cyber risk exposure and the management thereof to key stakeholders in integrated reports (Mazumder & Hossain 2023). On the other hand, reporters should concurrently caution against disclosing critical information that could be exploited by cybercriminals (Peng & Krivacek 2020).

Limited research has been conducted on cybersecurity disclosure internationally (Gao, Calderon & Tang 2020; Héroux & Fortin 2020; Sari et al. 2024). Given that South Africa has been identified as the most targeted African country (Interpol 2021), this exploratory study was conducted to investigate cybersecurity disclosure by selected companies listed on the Johannesburg Stock Exchange (JSE) that are most vulnerable to cyber threats. Cybersecurity disclosures by companies that were listed in the health care and Technology industries, and Retail and Banking sectors of the JSE between 2017 and 2022 were analysed. These industries and sectors are mainly affected by cyberattacks (Pieterse 2021). The sampled companies' cybersecurity disclosures were investigated pre- and during the COVID-19 pandemic to explore significant changes. Content analysis was conducted on their integrated reports based on the six-step approach outlined by Babbie (2021). Three cybersecurity disclosure metrics, namely disclosure presence, level and volume were considered. This study thereby makes a unique contribution by enabling corporate stakeholders to reflect on key cybersecurity matters in highly targeted South African industries and sectors based on disclosure presence (number of keyword occurrences), disclosure level (reflecting the variety of unique cybersecurity matters that were disclosed) and disclosure volume (paragraphs devoted to cybersecurity considerations). By identifying prominent issues on which highly targeted companies focused, policies and practices can be developed and refined to enhance cybersecurity. This is a key corporate governance consideration as technology, in particular artificial intelligence (AI), is developing at an unprecedented rate.

Since the advent of the COVID-19 pandemic, the sampled companies considerably enhanced their reporting on cyber-related information. Current and prospective shareholders can reflect on such disclosures to identify investee companies that have improved their cybersecurity, thereby arguably enhancing their legitimacy.

Cybersecurity considerations and relevant regulation are discussed next. Details are also provided on cybersecurity disclosure in the context of the legitimacy theory. Thereafter, the methodology is outlined, followed by a discussion on trends and significant differences for the three cybersecurity measures for the overall period and per annum. Lastly, conclusions and recommendations are offered for several corporate stakeholders.

Cybersecurity considerations, regulation and disclosure

Cyber risk refers to the possibility of disruption, reputational damage and monetary loss if IT systems fail (Aldasoro et al. 2022). Issues related to the use of information and communication technology (ICT) might further cause business disruption and infrastructure failure (Eling & Schnell 2016).

Given the rise of such cybersecurity concerns, cyber resilience is gaining prominence among corporate leaders and IT officials, as it reflects a company's capacity to plan for, react to and recover from cyber risks and attacks (Accenture 2021b). The changing workplace settings of employees who worked remotely when the COVID-19 pandemic occurred negatively impacted the cyber resilience of several companies globally (Soni, Kukreja & Sharma 2020).

Corporate leaders should thus ensure that cybersecurity and risk management are sufficiently integrated in corporate strategic objectives (Accenture 2021b; Maynard, Onibere & Ahmad 2018). Sound cyber risk management substantially enhances corporate capacity to identify, investigate, implement and monitor cyber risks (IT Governance 2022).

To assist them with cyber risk management, the boards of directors increasingly appoint a chief information security officer (CISO). The CISO's key role is to focus on technological developments and the related cybersecurity implications (Eling & Schnell 2016). Companies also appoint chief information officers (CIOs) and chief technology officers (CTOs) to assist them in accounting for internal and emerging technologies, respectively (McKinsey & Company 2023). These individuals would then regularly engage with the board and IT governance committee on key cybersecurity matters and the latest technological developments, in particular AI (Board Portal 2023). Focus is placed on prominent cyber risks and regulation in South Africa in the next section, given the scope of this study.

Prominent cyber risks and regulation in South Africa

South Africa is an attractive target for cybercriminals (Census and Economic Information Center Data 2022; Interpol 2021). The most prevalent cyber risks in the country include phishing, data leaks, ransomware, distributed denial-of-service (DDoS) attacks and compromised websites (Pieterse 2021; Van Niekerk 2017).

Phishing entails that malware is installed to give a hacker access to sensitive information by luring employees to click on a malicious link (Zwilling 2022). This type of cyber threat

often occurs in Banking and Health Care. Another costly cyber risk is data leaks. Client trust is broken, and legal action can be taken should sensitive data be exposed (Shekokar et al. 2022).

Ransomware is another prevalent cyber risk in the local context that can be used to encrypt confidential data. A ransom is then typically demanded from the victim company to regain access to the encrypted data (Institute of Chartered Accountants in England and Wales [ICAEW] 2016). Furthermore, a target's server can be flooded with internet traffic during a DDoS attack. Access to online services is then prevented and business operations come to a halt. Lastly, a website can become compromised if a hacker alters the code, thereby negatively affecting its availability, integrity and confidentiality (Pieterse 2021).

South Africa's public sector is particularly vulnerable to cyberattacks (Pieterse 2021). The amendment of the *Protection of Personal Information (POPI) Act* (*No. 4 of 2013*) makes provision for the impact of cybercrime on the personal information of South African citizens (Republic of South Africa 2022). This Act outlines that institutions that are in possession of personal data will be held liable for data breaches.

Furthermore, the *Cybercrimes Act* (*No. 19 of 2020*) came into effect in 2021 to establish a comprehensive cybersecurity legislative framework to deal with cybersecurity issues in the country. This Act outlines cyber-related legal offences, including unlawful access to and the interception of data, hacking and the use of ransomware. Cybercrime offenses can as such result in fines and imprisonment (Republic of South Africa 2021).

Given the rise in cyberattacks and the apparent weaknesses in IT security systems, the South African Reserve Bank's (SARB) Prudential Authority and the Financial Sector Conduct Authority (FSCA) released a joint draft standard on cybersecurity and cyber resilience requirements following the arrival of the COVID-19 pandemic. This joint standard was finalised in 2024 to ensure that local financial institutions have proper cybersecurity and cyber resilience procedures and systems (SARB 2024).

Furthermore, the King IV Report on corporate governance recommends that companies should disclose their cyber-, IT- and ICT management processes (IoDSA 2016). Principle 12 offers specific guidance on how to disclose information relating to IT: 'The governing body should govern Technology and information in a way that supports the organisation setting and achieving its strategic objectives' (IoDSA 2016). Details on cybersecurity should be disclosed to stakeholders in integrated reports.

Linking cybersecurity disclosure to the legitimacy theory

Cybersecurity disclosure specifically centres on a company's cyber risk exposure and the management thereof (Mazumder & Hossain 2023). Investors and other key stakeholders require sufficient disclosure on material matters, including cyber risks and related corporate actions to make informed decisions. Yet report preparers should be cognisant that cybersecurity disclosures that are too detailed might result in exploitation by cybercriminals (Peng & Krivacek 2020).

Internationally, limited research has been conducted on cybersecurity disclosure (Chen, Henry & Jiang, 2023; Gao et al. 2020; Héroux & Fortin 2020; Kurnia & Ardianto 2024; Sari et al. 2024). Most of these studies were conducted pre-2020. Héroux and Fortin (2020) conducted content analysis for Canadian companies between 2017 and 2018 and found that cybersecurity disclosure was low. Gao et al. (2020) further examined the content and linguistic characteristics of cybersecurity risk disclosures of listed companies in the United States between 2007 and 2018 and found that their risk disclosures became lengthy and increasingly difficult to read. Kurnia and Ardianto (2024) investigated the cybersecurity disclosures of banks in Indonesia. They compiled a cybersecurity disclosure score by conducting content analysis and largely ascribed the observed increase in cybersecurity disclosure to regulation.

Furthermore, Amir, Levi and Livne (2018) reported a negative link between cyberattacks and cybersecurity disclosure, as companies tend to limit reporting on such attacks. Yet Chen et al. (2023) noticed that cybersecurity risk disclosure only increased after a severe data breach. In addition, these authors recorded a significant negative market reaction if breached companies decreased their cybersecurity disclosures. The implication is that the market anticipates increased disclosure following a data breach.

Given the significance of cybersecurity disclosures as outlined by previous research, reporters should hence be transparent and provide verifiable cybersecurity disclosures. These disclosures have a considerable influence on stakeholders' attitudes towards and trust in reporting companies (Bansal & Axelton 2023). Furthermore, the perceived benefits of voluntary assurance on cyber disclosure, particularly if cybersecurity breaches occurred, significantly influence investors' judgements of the impacted companies (Navarro & Sutton 2024).

Investors often consult disclosures in integrated reports to reflect on key matters, such as cybersecurity. Such analyses of corporate disclosures are typically based on the legitimacy theory (Harymawan et al. 2020; Nuber & Velte 2021; Radu & Smaili 2021). Dowling and Pfeffer (1975) explained that corporate behaviour is substantively influenced by the views of stakeholders in the environment in which companies operate. To be perceived as legitimate a company's activities and the behaviour of its directors should be congruent with the values and beliefs of society. As South Africa is very vulnerable to cyberattacks, it is argued that corporate stakeholders will perceive companies that give more attention to cybersecurity as more legitimate than their counterparts that give less attention to this pressing matter.

Prior scholars outlined different types of legitimacy. Pragmatic legitimacy might specifically be gained through corporate disclosures (Suchman 1995). A company might obtain pragmatic legitimacy if it has the capacity to convince key stakeholders of its usefulness, inter alia, to protect their personal information (Bowen 2019).

Pragmatic legitimacy includes dispositional and exchange legitimacy. Dispositional legitimacy is acquired when companies are considered trustworthy and perceived to have their stakeholders' best interests at heart, given the assumptions that companies are autonomous and morally responsible actors (Suchman 1995). Similarly, exchange legitimacy refers to stakeholders supporting companies based on expected or realised benefits (Suchman 1995), such as the protection of their interests through enhancing cybersecurity. It is thus important that stakeholders gain a clear understanding of related corporate actions and implications through disclosures in integrated reports (Shehata 2014).

Methods

An exploratory study was conducted to investigate the cybersecurity disclosures of selected JSE-listed companies that are most vulnerable to cyberattacks by conducting content analysis. Qualitative information reported in the sampled companies' integrated reports were coded to analyse their cybersecurity disclosures. The sample was selected based on the following judgement criteria: a company had to operate in a sector or industry recognised for being exposed to cyberattacks and related risks; a company should have been listed on the JSE for at least 2 years from 2017 to 2022; and a company had to publish integrated reports while being listed.

Pieterse (2021), Reva (2021) and Van Niekerk (2017) found that Banking, Health Care and Retail companies were largely affected by cyberattacks. The Technology industry was furthermore selected as the use of technology, and consequently, cybercrime rose substantially during the recent pandemic (Dolley 2021; KPMG 2022). The research period hence covered the COVID-19 period (2020–2022) and the preceding 3 years (2017–2019). The sample comprised of 7 Banking, 8 Health Care, 23 Retail and 16 Technology companies.

Content analysis was conducted on the sampled companies integrated reports by adopting the six-step approach outlined by Babbie (2021). During Step 1, the operational definitions of the cybersecurity metrics were developed. The number of cybersecurity keyword occurrences were determined (denoted as disclosure presence). The number of unique cybersecurity keywords that were mentioned relative to the total number of unique keywords identified in Step 3 was then computed and converted to a percentage resulting in a coverage score (denoted as disclosure level). Lastly, the number of cybersecurity paragraphs per integrated report was determined (denoted as disclosure volume).

During Step 2, the researchers decided on the type of text media that they would observe, namely published integrated reports. Step 3 then entailed identifying applicable keywords during two phases. Firstly, the literature review resulted in the identification of unique cybersecurity keywords, mainly based on Mazumder and Hossain (2023), Pieterse (2021), Radu and Smaili (2021) and Van Niekerk (2017). Secondly, a pilot study was conducted to determine cybersecurity keywords that were specific to the local context, and the considered industries and sectors. As a result, 62 cybersecurity keywords were identified, as shown in Appendix 1. Keyword variations in terms of spelling and the usage of plural versus singular form as well as abbreviations versus words written in full also were considered.

During Steps 4 and 5, the required qualitative data were collected by conducting content analysis and coded by using AutoIt. This scripting program for Microsoft Windows utilises a Beginner's All-purpose Symbolic Instruction Code scripting language. AutoIt was used to convert the considered integrated reports into text files, similar to the method employed by Allini, Rossi and Hussainey (2016). The program mined 1 644 166 lines of text for the 62 cybersecurity keywords and their grammatical variations, as outlined in Step 3.

The program was furthermore scripted to determine 'false positives', that is, results that suggest the potential disclosure presence of cybersecurity keywords while they were used in other contexts, such as 'defend' in the context of unrelated risks. The outlined process resulted in the extraction of 10 821 data points along with their metadata, including the position of each cybersecurity keyword hit, and the surrounding text. The data were then imported in Google sheets where after the primary researcher checked that there were no remaining 'false positives'. The three cybersecurity measures indicated in Step 1 were then computed and captured in Microsoft Excel, whereafter the data were analysed and reported (Step 6).

Given that the research period included the COVID-19 pandemic, the researchers determined significant differences in the three cybersecurity disclosure metrics. A sequential analysis of variance (ANOVA) was used to explore significant differences over the entire research period while Fisher's least significant difference (LSD) test showed significant differences per year.

Pertaining to validity, the data were sourced from the audited integrated reports of the sampled companies. In terms of reliability, the six-step content analysis approach was outlined in detail and can be used by future researchers to conduct comparative studies.

Ethical considerations

Ethical clearance (exemption) was obtained from the relevant Departmental Ethics Screening Committee of Stellenbosch University before collecting the data. This article followed all ethical standards for research without direct contact with human or animal subjects.

Results and discussion

The outcomes of the content analysis in terms of disclosure presence, level and volume of cybersecurity will now be reported. Descriptive trends will be discussed first, followed by the outcomes of the difference tests.

Descriptive results

The disclosure presence is shown in Figure 1. The number of cybersecurity keyword occurrences increased noticeably post-2020, from 20 mean keyword occurrences in 2019 to 28 mean keyword occurrences in 2022. The maximum number of keyword occurrences was 109 in 2020 for a company that was a victim of a cyberattack. This attack resulted in the noticeable spike in disclosure presence of cybersecurity. Yet some sampled companies only disclosed 1 keyword, as indicated by the minimum value in Figure 1.

The sampled companies focused on specific keywords, thereby highlighting the most prominent cybersecurity matters. The most disclosed keywords for the overall sample were cybersecurity, IT and IT governance. Given the rise in cybercrime in South Africa, these keywords reflect noticeable awareness of the importance of cybersecurity. The extensive use of IT governance furthermore alludes to IT- and cyber-engagement from various of the sampled companies' boards, in line with Principle 12 of King IV (IoDSA 2016). Various of the companies, however, mentioned the keyword 'cyber' when disclosing details on security procedures and test breaches, instead of using the more nuanced 'cyber resilience'. Table 1 indicates the top 15 keywords used by the sampled companies per year.

A notable switch occurred in 2020 between the two most used keywords. A possible explanation for the prominent use of the keyword 'cybersecurity' could be the advent of the COVID-19 pandemic which triggered an unbridled level of cybercrime (Dolley 2021; Interpol 2021; KPMG 2022). The considered companies increasingly focused on cybersecurity as a top priority during the latter part of the study period. Information Technology or IT received substantial attention pre- and post-2020.

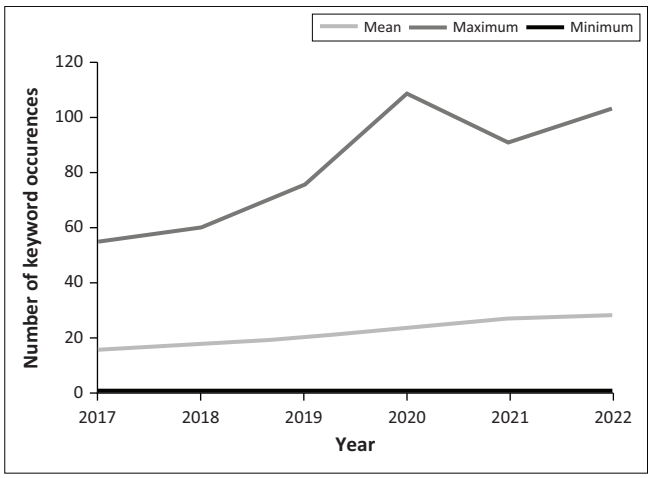

FIGURE 1: Disclosure presence of cybersecurity.

A possible reason for this trend could be the continuous introduction of new technologies (Côrte-Real et al. 2020), in particular AI which could provide competitive advantages that should be properly managed and reported on. Further, corporates must adapt their practices to reflect on the ever-changing cyberspace and IT environment to ensure survival. Consequently, IT governance remained in third position from 2018 to 2022. In 2017, King IV came into effect and, among others, promoted the importance of IT governance in Principle 12 (IoDSA 2016). The popularity of this keyword could thus be partly linked to the sampled companies' attempts to adhere to this principle.

Integrated reporting should provide risk and opportunity-related disclosures in the context of divergent capitals, including intellectual capital (International Financial Reporting Standards 2021). References to intellectual capital in cybersecurity disclosures gradually gained prominence in the analysed integrated reports. This keyword moved to the fourth position in 2022, as shown in Table 1. The increased use of the term intellectual capital could indicate that the sampled companies gradually broadened their focus of this capital given rapid technological developments.

Cyber resilience only appeared in the list of top 15 keywords in 2022. This development shows that the considered companies became more aware of the need for cyber resilience following the advent of the COVID-19 pandemic and the discussed increase in legislation. Peter (2017) likewise suggested that cyber resilience is crucial to fully realise e-commerce and to ensure corporate continuity. Table 2 shows the top 15 keywords per industry or sector for the overall period.

As depicted in Table 2, cybersecurity was an overarching concern for all considered industries and sectors. The Banking sector had a particularly strong focus on cybercrime, IT and cyber risks. Given that the South African Banking sector predominantly operates in cyberspace, their focus on possible cyber risks and crimes was expected. A cyberattack and breach of a bank's security could result in substantial financial losses for several stakeholders. The draft joint standard on cybersecurity and cyber resilience that is applicable to this sector most likely also contributed to their focus on cyber risk, fraud and disruption (SARB 2024).

The considered Health Care companies placed substantial emphasis on information security and related governance considerations. Four commonly used keywords contained the word security, namely cybersecurity, information security, IT security and data security. The focus on information security could be largely ascribed to their collection and sharing of confidential patient information online and across networks. Furthermore, the need to access patient data at any time, especially in emergency situations, implies that hospitals should have a very reliable cybersecurity framework (Cyber Security Institute 2023).

TABLE 1: Top 15 disclosed keywords per annum based on the number of keyword occurrences (*n*).

Position	2017		2018		2019		2020		2021		2022	
	Keywords	*n*	Keywords	*n*	Keywords	*n*	Keywords	*n*	Keywords	*n*	Keywords	*n*
1	Information technology	134	Information technology	101	Information technology	128	Cybersecurity	223	Cybersecurity	307	Cybersecurity	307
2	IT governance	93	Cybersecurity	93	Cybersecurity	121	Information technology	136	Information technology	121	Information technology	135
3	Cybersecurity	70	IT governance	90	IT governance	91	IT governance	106	IT governance	100	IT governance	94
4	ICT	69	ICT	72	Information security	76	Cyber	69	Information security	84	Intellectual capital	80
5	Cybercrime	42	Information security	59	ICT	71	Information security	66	Protection of personal information	66	Information security	79
6	Information security	36	IT risk	55	IT risk	52	Intellectual capital	56	Intellectual capital	62	Cyber	76
7	Information management	30	Intellectual capital	41	Intellectual capital	50	Protection of personal information	51	ICT	60	Cyber risk	60
8	Intellectual capital	28	Cybercrime	37	Cyber risk	43	Cyberattack	50	Cyber	59	Protection of personal information	59
9	Cyber	27	Protection of personal information	36	Information management	42	ICT	47	IT risk	52	Data security	50
10	IT security	27	Information management	33	Protection of personal information	38	Data security	47	Data security	51	Cyber resilience	40
11	IT risk	26	Cyber	29	Cybercrime	37	IT risk	46	Cyber risk	49	Cybercrime	40
12	Protection of personal information	25	IT security	27	Cyber	35	Information management	39	Cyberattack	40	ICT	39
13	Cyber risk	25	Cyber risk	26	IT security	33	Cybercrime	35	Information management	37	Cyberattack	39
14	Data security	17	Data security	16	Data security	19	Attack	35	Cyber threat	35	IT security	32
15	Disruption	17	Cyberattack	15	Disruption	17	Cyber risk	31	Cybercrime	32	Phishing	27

IT, information technology; ICT, information and communication technology.

TABLE 2: Top 15 disclosed keywords per industry/sector based on the number of keyword occurrences (*n*).

Position	Banking sector		Health Care industry		Retail sector		Technology industry	
	Keywords	*n*	Keywords	*n*	Keywords	*n*	Keywords	*n*
1	Cybersecurity	246	Cybersecurity	229	Information technology	364	Cybersecurity	454
2	Information technology	216	ICT	210	IT governance	336	Information technology	104
3	IT risk	160	Information security	130	Cybersecurity	214	ICT	102
4	Cyber risk	136	IT governance	102	Intellectual capital	105	Cyber	95
5	Cybercrime	134	Information technology	94	Protection of personal information	97	IT governance	90
6	Cyber	134	Intellectual capital	85	Information security	93	Data security	78
7	Information security	106	Information management	71	Information management	75	Information security	75
8	Protection of personal information	64	Cybercrime	67	Cyber risk	72	Intellectual capital	71
9	Intellectual capital	65	Protection of personal information	47	Cyberattack	64	Protection of personal information	71
10	Technology risk	56	Cyberattack	46	Data security	60	IT security	61
11	Disruption	52	IT security	44	IT security	58	Cyber resilience	50
12	IT governance	47	Data security	44	Cyber	41	Information management	49
13	Attack	40	Cyber	42	IT risk	40	IT risk	45
14	Digital fraud	34	Attack	20	Cyber threat	38	ICT security	44
15	Disruptive technologies	31	Cyber threat	20	Disruption	38	Phishing	44

IT, information technology; ICT, information and communication technology.

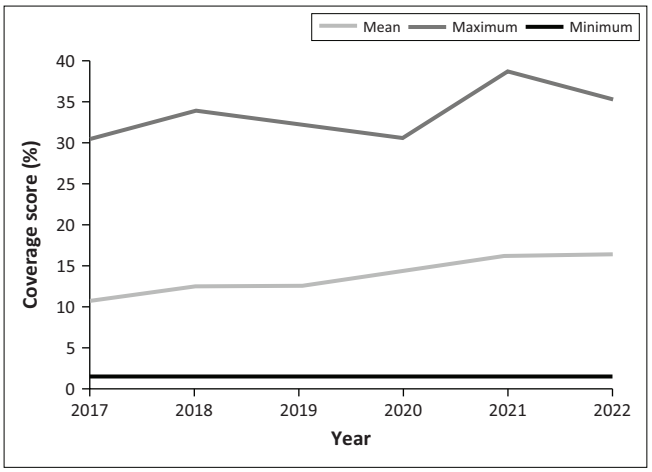

FIGURE 2: Disclosure level of cybersecurity.

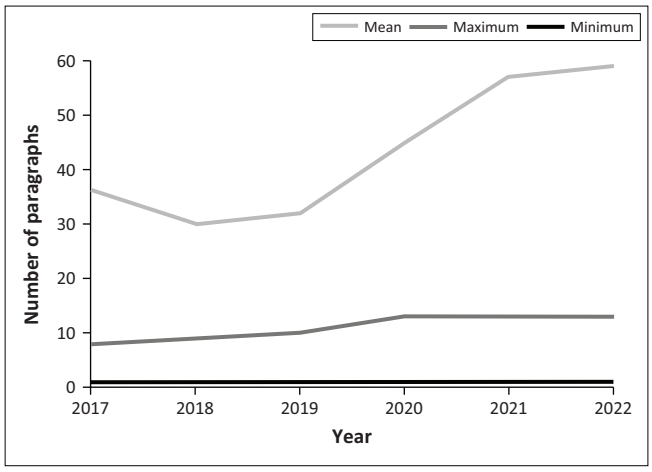

FIGURE 3: Disclosure volume of cybersecurity.

The Retail sector also had a strong focus on information security and the protection of personal information. Retailers often have loyalty card systems in place, as well as credit facilities. Thus, many retailers regularly collect private information from customers. A breach in a retailer's IT systems could not only result in the loss or theft of customer data but also the loss of customer trust and loyalty (Interpol 2023).

Notably, the Technology industry was the only industry that had cyber resilience in its top 15 keywords. Furthermore, the top five keywords for this industry were systems-orientated, as the keywords cybersecurity, IT, ICT, cyber and IT governance strongly relate to cyber-systems, frameworks and infrastructure. This industry's strong links to the recent developments in cyberspace contributed to this disclosure focus. Figure 2 shows the descriptive results for the disclosure level of cybersecurity, based on the number of disclosed keywords as a percentage of the considered 62 keywords (coverage scores).

Based on the 2017 mean of 10.85%, the sampled companies used on average between six and seven different cybersecurity-related keywords when reporting on cyber matters. In contrast, by 2022 they used about 10 keywords, as shown by the mean of 16.38% in Figure 2. The company that used 24 different cybersecurity-related keywords in their integrated report (as indicated by the maximum score of 38.71% in 2021) emphasised cyber resilience.

Yet the minimum value of 1.61% indicates that a sampled company only used one cybersecurity-related keyword in their integrated reports. This company briefly referred to 'cybersecurity' but did not mention any of the other keywords. Figure 3 provides the descriptive statistics for the disclosure volume, based on the number of paragraphs containing cybersecurity keywords.

An increase is also observed in the mean number of paragraphs comprising cybersecurity keywords over the duration of the research period, as shown in Figure 3. Yet there was substantial deviation in the number of paragraphs, as seen by the maximum and minimum values. Given that South Africa is a prime target for cyberattacks, the need for cybersecurity is heightened (Interpol 2021).

The King IV Report (IoDSA 2016) furthermore guides JSE-listed companies in terms of cybersecurity disclosures, thereby possibly contributing to the observed increase in disclosure volume of cybersecurity since its publication in 2017. By 2022, the average number of paragraphs were 13 versus 8 in 2017. In contrast, Radu and Smaili (2021) reported that Canadian firms had approximately five cybersecurity-related paragraphs per analysed integrated report pre-2020.

The Technology industry showed the largest increase in the number of cybersecurity-related paragraphs. As Technology companies are primary users and providers of IT and cyberspace services, the considered Technology companies arguably enhanced their disclosures given the rapidly developing cyber-related risks and security concerns post-2020.

Outcomes of the difference tests

The outcomes of the sequential ANOVA and the Fisher's LSD tests show the significance of the observed trends for disclosure presence over the entire period and per annum in Table 3 and Table 4, respectively.

As seen in Table 3, the mean number of cybersecurity keyword occurrences in the analysed integrated reports differed significantly over the entire research period (F-value: 4.51; p-value: 0.00). No significant differences occurred in the average number of cybersecurity-related keyword occurrences before the onset of the COVID-19 pandemic, as shown by the p-value of 0.16 for the difference between 2017 and 2018, and the p-value of 0.19 for the difference between 2018 and 2019 in Table 4. Yet post-2020, most of the annual differences were significant. Further investigation showed that these significant differences were ascribed to increases of three or more cybersecurity-related keyword occurrences per annum.

Scholars and practitioners confirm that cybercrime increased drastically given the increased use of cyberspace in business operations since 2020 (Dolley 2021; KPMG 2022). The COVID-19 pandemic practically forced companies to accelerate their adoption of Technology and cyberspace in their day-to-day business activities (Soni et al. 2020).

A growing number of the sampled companies evidently enhanced their disclosures on prevalent and material cyber risks, and the security-related implications post-2020 to ultimately enhance their legitimacy (Suchman 1995). Such companies showcased to their stakeholders that they have given due consideration to cybersecurity matters, thereby protecting private information and enhancing data security.

The outcomes of the ANOVA and Fisher's LSD analyses for disclosure level (mean coverage scores) for the overall period and annual differences are provided in Table 5 and Table 6, respectively.

TABLE 3: Difference test for disclosure presence (overall period): ANOVA (mean number of keyword occurrences for the overall period).

Effect	ANOVA (mean number of keyword occurrences during the overall period)			
	Numerator degrees of freedom	Denominator degrees of freedom	*F*-value	*p*-value
(Intercept)	1	250	105.18***	0.01
Year	5	250	4.51***	0.00

ANOVA, analysis of variance.
***, significant at the 1% level.

TABLE 4: Difference test for disclosure presence (annual differences).

Year	Fisher's LSD (mean number of keyword occurrences per year)				
	2018	2019	2020	2021	2022
2017	0.16	0.03**	0.00***	0.00***	0.00***
2018	-	0.19	0.00***	0.00***	0.00***
2019	-	-	0.02**	0.00***	0.01***
2020	-	-	-	0.09*	0.21
2021	-	-	-	-	0.94

LSD, least significant difference.
*, significant at the 10% level; **, significant at the 5% level; ***, significant at the 1% level.

TABLE 5: Difference test for disclosure level (entire research period).

Effect	ANOVA (conducted on the mean coverage score for the overall period)			
	Numerator degrees of freedom	Denominator degrees of freedom	*F*-value	*p*-value
(Intercept)	1	250	223.26***	< 0.01
Year	5	250	5.96***	< 0.01

ANOVA, analysis of variance.
***, significant at the 1% level.

TABLE 6: Difference test for disclosure level (yearly differences).

Year	Fisher's LSD (mean coverage scores per annum)				
	2018	2019	2020	2021	2022
2017	< 0.01***	0.03**	< 0.01***	< 0.01***	< 0.01***
2018	-	0.79	0.06*	< 0.01***	< 0.01***
2019	-	-	0.03**	< 0.01***	< 0.01***
2020	-	-	-	< 0.01***	0.07*
2021	-	-	-	-	0.80

LSD, least significant difference.
*, significant at the 10% level; **, significant at the 5% level; ***, significant at the 1% level.

The disclosure level of cybersecurity also differed significantly over the entire research period (*F*-value: 5.96; *p*-value: < 0.01) as shown in Table 5, similar to the results reported for disclosure presence in Table 3. Furthermore, most of the yearly differences in the coverage score were statistically significant, as indicated in Table 6. When the COVID-19 pandemic emerged, many companies lacked appropriate cybersecurity systems to facilitate safe and effective remote working. Several companies consequently fell prey to cyberattacks and cybercrimes. Unique cyber risks also became more prevalent (PwC 2022). Post-2020, the sampled companies consequently expanded their reporting on unique cybersecurity matters, as shown by the significant differences in their coverage scores in Table 6.

The non-significant differences between 2018 and 2019 (*p*-value: 0.79) and 2021 and 2022 (*p*-value: 0.80) are ascribed to the minimal changes in the mean coverage scores during these years. The descriptive outcomes show that the mean coverage score only increased with 0.17% between 2018 and 2019, while there was only a 0.01% increase in the mean coverage score from 2021 to 2022. The outcomes of the difference tests for disclosure volume of cybersecurity are provided in Table 7 and Table 8 for the overall period and per annum, respectively.

Perusal of Table 7 shows that the average number of paragraphs containing cybersecurity keywords also increased noticeably over the entire period under review (*F*-value: 3.24; *p*-value: 0.01). Given the escalation in cybercrime following the onset of the COVID-19 pandemic (Dolley 2021; Interpol 2021; KPMG 2022), the significant difference from 2019 to 2020 (*p*-value: 0.00) in Table 8 was not unexpected. Figure 3 shows that the mean disclosure volume increased substantially between 2019 (10 paragraphs) and 2020 (13 paragraphs covering cybersecurity content).

Yet the average number of paragraphs then remained at 13 in 2021 and 2022, as shown in Figure 3. As such, no significant

TABLE 7: Difference test for disclosure volume (overall period).

Effect	ANOVA (mean number of paragraphs for the overall period)			
	Numerator degrees of freedom	Denominator degrees of freedom	*F*-value	*p*-value
(Intercept)	1	250	81.67***	0.01
Year	5	250	3.24***	0.01

ANOVA, analysis of variance.
***, significant at the 1% level.

TABLE 8: Difference test for disclosure volume (yearly differences).

Year	Fisher's LSD (mean number of paragraphs per annum)				
	2018	2019	2020	2021	2022
2017	0.23	0.05**	0.00***	0.00***	0.00***
2018	-	0.18	0.00***	0.00***	0.01***
2019	-	-	0.00***	0.01***	0.05**
2020	-	-	-	0.65	0.96
2021	-	-	-	-	0.70

LSD, least significant difference.
, significant at the 5% level; *, significant at the 1% level.

differences were observed between 2020 and 2021 (p-value: 0.65), and 2021 and 2022 (p-value: 0.70) in Table 8. Based on these results, stakeholders' reporting demands were arguably already met in terms of disclosure volume in 2020, thereby enhancing the sampled companies' pragmatic legitimacy (Suchman 1995). Post-2020, the sampled companies then expanded their focus to ensure that unique cybersecurity matters receive sufficient attention, as shown by the significant annual differences in the coverage scores in Table 6.

Conclusion and recommendations

The rise in cyberattacks and crimes resulted in increased corporate focus on cybersecurity worldwide. The effects of poor cybersecurity in South Africa carry dire and far-reaching consequences for companies and their stakeholders. Corporate leaders should hence duly account for the integration of cybersecurity within their strategies.

The *Cybercrimes Act* (*No. 10 of 2020*) was introduced to improve cyber resilience in South Africa. The King IV Report furthermore provides recommendations on Technology and information matters to corporate leaders. Given that corporate strategies are developed by boards of directors, sound corporate governance imply that boards have considered the impact of cybersecurity risks. They should further ensure that sufficient information is disclosed to stakeholders in line with the legitimacy theory.

This study was conducted to explore the disclosure presence, level and volume of cybersecurity disclosure by selected JSE-listed companies that were most likely to be targeted over the period 2017 to 2022. Content analysis was conducted on the sampled companies' integrated reports based on 62 keywords. Sequential ANOVA and Fisher's LSD tests were conducted to determine significant differences over the entire research period and per annum, respectively.

The descriptive results indicated that the sampled companies increasingly focused on cybersecurity matters. Cybersecurity disclosure increased noticeably in 2020, given the external shock of the COVID-19 pandemic and the resultant rise in cybercrime. KPMG (2022) confirmed that companies rapidly adopted and adapted cyber practices when the pandemic occurred.

The disclosure level of cybersecurity revealed noticeable variations in the reporting habits and related focus areas of the sampled companies. The most disclosed keywords included cybersecurity and IT governance. Towards the end of the research period, more nuanced cybersecurity-related keywords were used, including cyber resilience. Pertaining to the disclosure volume of cybersecurity, the mean number of paragraphs increased from 8 in 2017 to 13 paragraphs in 2020, whereafter it remained stagnant.

Statistically significant differences were observed for the disclosure presence, level and volume of cybersecurity over the entire research period. Given the disconcerting risk of being targeted by cybercriminals in South Africa, companies that significantly enhanced their cybersecurity disclosures are likely to improve their legitimacy if they evidently focused on the protection of private information and data security. Most of the annual differences in the disclosure presence of cybersecurity were statistically significant. Yet the differences in the disclosure volume of cybersecurity in 2020, 2021 and 2022 were non-significant as the average number of cybersecurity-related paragraphs plateaued from 2020 onwards. The sampled companies focused on enhancing their coverage post-2020 by reporting on a broader range of unique cybersecurity matters than during 2017–2019.

Based on the reported results, it is recommended that the IoDSA provide more in-depth guidelines for cybersecurity risk management. Directors should constantly explore emerging cyber risks as Technology continues to develop at an unprecedented rate. Directors are further encouraged to regularly attend cybersecurity seminars and utilise training opportunities to stay abreast of potential solutions for threats. If directors within the considered industries and sectors do not give sufficient attention to prominent cyber risks and security concerns as outlined in this study, it could be deemed an infringement of their duty of care.

Pertaining to the limitations of this research, the sample only included a limited number of companies from selected JSE industries and sectors that were largely affected by cybercrime. The sample further largely comprised Retail companies. The findings are hence not generalisable to the entire JSE. Future researchers could conduct a similar study by including more industries over a longer time frame for a range of emerging markets. The metrics (disclosure presence, level, volume) are furthermore descriptive proxies. While content analysis was conducted for the purpose of this study, interviews could hence be conducted with directors and IT officials to explore the quality and nuance of corporate cybersecurity disclosures.

Acknowledgements

This article is based on research originally conducted as part of Laura F. Putter's master's thesis titled 'The relationship between board gender diversity and cybersecurity disclosure: An emerging market perspective', submitted to the Economic and Management Sciences, Department of Business Management, Stellenbosch University in 2023. The thesis is currently unpublished and not publicly available. The thesis was supervised by Mrs Ruth Johnson and Prof. Nadia Mans-Kemp. The manuscript has been revised and adapted for journal publication. The author confirms that the content has not been previously published or disseminated and complies with ethical standards for original publication.

Competing interests

The authors declare that they have no financial or personal relationships that may have inappropriately influenced them in writing this article.

CRediT authorship contribution

Laura F. Putter: Conceptualisation, Methodology, Investigation, Writing – original draft, Software, Writing – review & editing. Ruth Johnson: Conceptualisation, Writing – original draft, Writing – review & editing, Supervision. Nadia Mans-Kemp: Conceptualisation, Writing – original draft, Writing – review & editing, Supervision. All authors reviewed the article, contributed to the discussion of results, approved the final version for submission and publication, and take responsibility for the integrity of its findings.

Funding information

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Data availability

The authors declare that all data that support this research article and findings are available in the article and its references.

Disclaimer

The views and opinions expressed in this article are those of the authors and are the product of professional research. It does not necessarily reflect the official policy or position of any affiliated institution, funder, agency, or that of the publisher. The authors are responsible for this article's findings, and content.

References

Accenture, 2021a, *2021 cyber threat intelligence report*, viewed 16 February 2025, from https://www.accenture.com/content/dam/accenture/final/a-com-migration/pdf/pdf-172/accenture-2021-cyber-threat-intelligence-report.pdf.

Accenture, 2021b, *State of cybersecurity resilience 2021: How aligning security and the business creates cyber resilience*, viewed 16 February 2025, https://www.accenture.com/content/dam/accenture/final/a-com-migration/pdf/pdf-165/accenture-state-of-cybersecurity-2021.pdf.

Aldasoro, I., Gambacorta, L., Giudici, P. & Leach, T., 2022, 'The drivers of cyber risk', *Journal of Financial Stability* 60, 1–13. https://doi.org/10.1016/j.jfs.2022.100989

Allini, A., Rossi, F.M. & Hussainey, K., 2016, 'The board's role in risk disclosure: An exploratory study of Italian listed state-owned enterprises', *Public Money and Management* 36(2), 113–120. https://doi.org/10.1080/09540962.2016.1118935

Amir, E., Levi, S. & Livne, T., 2018, 'Do firms underreport information on cyber-attacks? Evidence from capital markets', *Review of Accounting Studies* 23(3), 1177–1206. https://doi.org/10.1007/s11142-018-9452-4

Babbie, E.R., 2021, *The practice of social research*, 15th edn., Cengage Learning, Boston, MA.

Bansal, G. & Axelton, Z., 2023, 'Impact of cybersecurity disclosures on stakeholder intentions', *Journal of Computer Information Systems* 64(1), 78–91. https://doi.org/10.1080/08874417.2023.2180785

Board Portal, 2023, *Understanding the IT governance board: Composition, responsibilities, and best practices*, viewed 10 October 2023, from https://board-room.org/blog/it-governance-board/.

Bowen, F., 2019, 'Marking their own homework: The pragmatic and moral legitimacy of industry self-regulation', *Journal of Business Ethics* 156(1), 257–272. https://doi.org/10.1007/s10551-017-3635-y

Bravo, F., 2017, 'Are risk disclosures an effective tool to increase firm value?', *Managerial and Decision Economics* 38(8), 1116–1124. https://doi.org/10.1002/mde.2850

Census and Economic Information Center Data, 2022, *South Africa market capitalisation*, viewed 09 September 2022, from https://www.ceicdata.com/en/indicator/south-africa/market-capitalization.

Chen, J., Henry, E. & Jiang, X., 2023, 'Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach', *Journal of Business Ethics* 187, 199–224. https://doi.org/10.1007/s10551-022-05107-z

Clinton, L., 2022, *Cybersecurity for business organization: Wide strategies to ensure cyber risk is not just an IT issue*, Kogan Page, London.

Côrte-Real, N., Ruivo, P. & Oliveira, T., 2020, 'Leveraging Internet of Things and big data analytics initiatives in European and American firms: Is data quality a way to extract business value?', *Information and Management* 57(1), 1–16. https://doi.org/10.1016/j.im.2019.01.003

Craigen, D., Diakun-Thibault, N. & Purse, R., 2014, 'Defining cybersecurity', *Technology Innovation Management Review* 4(10), 13–21. https://doi.org/10.22215/timreview835

Cyber Security Institute, 2023, *Cyber security and the South African Healthcare industry during COVID-19*, viewed 06 September 2023, from https://cybersecurityinstitute.co.za/cyber-security-and-the-south-african-healthcare-industry-during-covid-19/.

Dolley, C., 2021, 'Cyberattacks: South Africa, you've been hacked', *Daily Maverick*, 06 November, viewed 17 February 2025, from https://www.dailymaverick.co.za/article/2021-11-06-cyberattacks-south-africa-youve-been-hacked/.

Dowling, J. & Pfeffer, J., 1975, 'Organizational legitimacy: Social values and organizational behavior', *Pacific Sociological Review* 18(1), 122–136. https://doi.org/10.2307/1388226

Eling, M. & Schnell, W., 2016, 'What do we know about cyber risk and cyber risk insurance?', *Journal of Risk Finance* 17(5), 474–491. https://doi.org/10.1108/JRF-09-2016-0122

Gao, L., Calderon, T.G. & Tang, F., 2020, 'Public companies' cybersecurity risk disclosures', *International Journal of Accounting Information Systems* 38, 100468. https://doi.org/10.1016/j.accinf.2020.100468

Harymawan, I., Rahayu, N.K., Larasati, D.A., Ghofar, A. & Agustia, D., 2020, 'Insights into research on carbon disclosure', *Journal of Security and Sustainability Issues* 9(4), 1157–1164. https://doi.org/10.9770/jssi.2020.9.4(3)

Héroux, S. & Fortin, A., 2020, 'Cybersecurity disclosure by the companies on the S&P/TSX 60 index', *Accounting Perspectives* 19(2), 73–100. https://doi.org/10.1111/1911-3838.12220

Institute of Chartered Accountants in England and Wales (ICAEW), 2016, *Top five cyber risks*, viewed 13 August 2024, from https://www.icaew.com/-/media/corporate/files/technical/business-and-financial-management/smes/bas-files/top-five-cyber-risks.ashx.

Institute of Directors South Africa (IoDSA), 2016, *Report on corporate governance for South Africa 2016*, viewed 19 June 2024, from https://www.adams.africa/wp-content/uploads/2016/11/King-IV-Report.pdf.

International Financial Reporting Standards, 2021, *International <IR> framework*, viewed 18 August 2024, from https://integratedreporting.org/wp-content/uploads/2021/01/InternationalIntegratedReporting Framework.pdf.

Interpol, 2021, *African cyberthreat assessment report*, viewed 17 May 2023, from https://www.interpol.int/content/download/16759/file/AfricanCyberthreat Assessment_ENGLISH.pdf.

Interpol, 2023, *African cyberthreat assessment report: Cyberthreat trends*, viewed 17 May 2023, from https://www.interpol.int/en/content/download/19174/file/2023_03CYBER_AfricanCyberthreat Assessment Report 2022_EN.pdf.

IT Governance, 2022, *IT governance's cyber resilience framework*, viewed 20 September 2024, from https://www.itgovernance.co.uk/cyber-resilience-framework.

KPMG, 2022, *Africa cybersecurity outlook 2022 survey*, viewed 20 August 2023, from https://kpmg.com/ke/en/home/insights/2022/09/Africa%20Cyber%20Outlook%20launch.html#:~:text=KPMG%20Africa%20today%20launched%20the,adequate%20investments%20in%20protecting%20assets.

Kurnia, P. & Ardianto, A., 2024, 'Board gender diversity and cyber security disclosure in the Indonesian banking industry: A two-tier governance context', *Corporate Governance* 24(7), 1614–1637. https://doi.org/10.1108/CG-01-2023-0010

Maynard, S.B., Onibere, M. & Ahmad, A., 2018, 'Defining the strategic role of the chief information security officer', *Pacific Asia Journal of the Association for Information Systems* 10(3), 61–86. https://doi.org/10.17705/1pais.10303

Mazumder, M.M.M. & Hossain, D.M., 2023, 'Voluntary cybersecurity disclosure in the banking industry of Bangladesh: Does board composition matter?', *Journal of Accounting in Emerging Economies* 13(2), 217–239. https://doi.org/10.1108/JAEE-07-2021-0237

McKinsey & Company, 2023, *What are the responsibilities of a CIO versus a CTO?*, viewed 04 November 2024, from https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-the-responsibilities-of-a-cio-versus-a-cto.

Navarro, P. & Sutton, S.G., 2024, 'Leveraging emerging cybersecurity reporting regulations: The effect of industry driven expectations for voluntary assurance', *Accounting Horizons* 39(1), 1–16. https://doi.org/10.2308/HORIZONS-2023-088

Nuber, C. & Velte, P., 2021, 'Board gender diversity and carbon emissions: European evidence on curvilinear relationships and critical mass', *Business Strategy and the Environment* 30(4), 1958–1992. https://doi.org/10.1002/bse.2727

Peng, J. & Krivacek, G., 2020, 'The growing role of cybersecurity disclosures', *Information Systems Audit and Control Association Journal* 1, 1–7.

Peter, A.S., 2017, 'Cyber resilience preparedness of Africa's top-12 emerging economies', *International Journal of Critical Infrastructure Protection* 17, 49–59. https://doi.org/10.1016/j.ijcip.2017.03.002

Pieterse, H., 2021, 'The cyber threat landscape in South Africa: A 10-year review', *African Journal of Information and Communication* 28(28), 1–21. https://doi.org/10.23962/10539/32213

PricewaterhouseCoopers (PwC), 2022, *PwC's global economic crime and fraud survey 2022*, viewed 22 September 2024, from www.pwc.com/fraudsurvey.

Radu, C. & Smaili, N., 2021, 'Empowering women: The role of emancipative forces in board gender diversity', *Journal of Business Ethics* 177(2), 351–374. https://doi.org/10.1007/s10551-020-04717-9

Republic of South Africa, 2021, *Cybercrimes Act 19 of 2022*, viewed 15 July 2024, from http://www.nsw.gov.au/sites/default/files/Government_Gazette_2_December.pdf#page=15.

Republic of South Africa, 2022, *Protection of Personal Information Act (POPI Act)*, viewed 16 September 2024, from https://popia.co.za.

Reva, D., 2021, *Cyber attacks expose the vulnerability of South Africa's ports*, Institute for Security Studies, viewed 13 September 2023, from https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports.

Sari, L., Adam, M., Fuadah, L.L. & Yusnaini, Y., 2024, 'Determinant factors of cyber security disclosure: A systematic literature review', *KnE Social Sciences* 9(14), 387–398. https://doi.org/10.18502/kss.v9i14.16113

Shehata, N.F., 2014, 'Theories and determinants of voluntary disclosure', *Accounting and Finance Research* 3(1), 18–26. https://doi.org/10.5430/afr.v3n1p18

Shekokar, N., Vasudevan, H., Durbha, S., Michalas, A., Nagarhalli, T., Mangrulkar, R. et al., 2022, *Cyber security threats and challenges facing human life*, CRC Press, Boca Raton, FL.

Soni, V., Kukreja, D. & Sharma, D.K., 2020, 'Security vs. flexibility: Striking a balance in the pandemic era', in R.K. Sharma (ed.), *2020 Institute of Electrical and Electronics Engineers (IEEE) International Conference on advanced networks and telecommunications systems*, New Delhi, IEEE, pp. 1–6, December 14–17th.

South African Reserve Bank (SARB), 2024, *Joint communication 2 of 2024 – Publication of the joint standard – Cybersecurity and cyber resilience*, viewed 02 November 2024, from https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-public-awareness/Communication/2024/Joint-Communication-2-of-2024-Publication-of-the-Joint-Standard-Cybersecurity-and-cyber-resilience.

Suchman, M.C., 1995, 'Managing legitimacy: Strategic and institutional approaches', *Academy of Management Review* 20(3), 571-610. https://doi.org/10.5465/amr.1995.9508080331

Van Niekerk, B., 2017, 'An analysis of cyber-incidents in South Africa', *African Journal of Information and Communication* 20, 113–132. https://doi.org/10.23962/10539/23573

World Economic Forum, 2022, *The global risks report 2022*, viewed 19 October 2023, from https://www.weforum.org/reports/global-risks-report-2022.

Zwilling, M., 2022, 'Trends and challenges regarding cyber risk mitigation by CISOS: A systematic literature and experts' opinion review based on text analytics', *Sustainability* 14(3), 1–29. https://doi.org/10.3390/su14031311

Appendix starts on the next page →

Appendix 1

Cybersecurity keywords

Antivirus
Attack
best practice technologies
CISO
Cyber
cyber incident
cyber insurance
cyber penetration
cyber resilience
cyber risk
cyber threat
Cyberattack
Cybercrime
Cybersecurity
cybersecurity attack
data leakage
data mismanagement
data security
data theft
Decrypt
Defend
digital attack
digital fraud
digital intervention
digital security
Disruption
disruptive technologies
distributed denial-of-service
Encrypt
financial crime risk
Firewall
Hacking
ICT
ICT governance
ICT risk
ICT security
information and communication
information management
information risk
information security
information technology
insider threat
intellectual capital
IT governance
IT infrastructure
IT risk
IT security
Malware
network security
online fraud
online security
Penetration
Phishing
protection of personal information
Ransomware
secure network
security breach
technology disruption
technology risk
technology security
threat detection
unauthorised access