Journal of Contemporary Management
Volume 23 Issue 1

Modelling a strategic cybersecurity management process

DOI: https://doi.org/10.35683/jcman1197.328

LOUISA TJELELE
Department of Auditing, University of Pretoria, South Africa
Email: louisa.tjelele@tuks.co.za
ORCID: https://orcid.org/0009-0002-7627-1272

BLANCHE STEYN*
Department of Auditing, University of Pretoria, South Africa
Email: blanche.steyn@up.ac.za
ORCID: https://orcid.org/0000-0003-0632-6346
*corresponding author

ABSTRACT

Purpose of the study: This study models an organisation's strategic cybersecurity management process. Organisations need a responsive strategic cybersecurity process to defend against and manage exposure to dynamic and evolving cybersecurity threats.

Design/methodology/approach: The modelling process used semi-structured interviews with interpretive structural modelling to link the interrelationships between seven strategic cybersecurity elements into a strategic process.

Findings: The results show cybersecurity governance and third-party security risks as the two dependent elements. While the interactive nature of the remaining five elements: technological infrastructure, resources and capabilities, collaboration among departments, secured information flow, cybersecurity training and awareness, classified them as linking elements to support the dependent elements.

Recommendations/value: Modelling assists managers in conceptualising non-typical processes that cut across departments or functions to document the link between elements for a more effectively optimised strategic process. The mix between formal (cybersecurity governance) and informal (collaboration among departments) elements assists in optimising the process. Using interpretive structural modelling contributes to the literature on strategic processes modelling in South Africa.

Managerial implications: Understanding the strategic cybersecurity process and its use of formal and informal elements in an organisation can improve the strategic alignment between the business and cybersecurity for more responsive risk decisions.

Keywords: Cybersecurity management; cybersecurity process; cybersecurity; interpretive structural modelling; strategic process; strategic process modelling.

Copyright: © 2026 by the authors. Open access under the terms and conditions of the Creative Commons Attribution (CC BY 4.0) license https://creativecommons.org/licenses/by/4.0/).

JEL Classification: D81

1. INTRODUCTION

In light of the escalation of cyber-related incidents, cybersecurity remains a key risk (Pieterse, 2021) for all business entities connected to the Internet. In the digital transformation of business processes (courtesy of Industry 4.0) and the shift to wireless and cloud computing (Matsepe & van der Lingen, 2022), unmonitored and under-monitored network access points leave businesses open to cyber threats that require an increasingly responsive strategic cybersecurity management process. Thus, effective cybersecurity needs to be supported by a strategic cybersecurity process (Savaş & Karataş, 2022). In an organisation, cybersecurity must be managed responsively (almost in real time) to adapt effectively to evolving cyber threats and achieve constant cybersecurity.

The persistence of cyber threats underscores the need for a responsive process (van Steen, 2025). This is supported by the 2024 South African national cybersecurity survey that found that 47% of the participating organisations reported experiencing between one and five cybersecurity incidents in the previous year, with 90% admitting to multiple breaches (Mtsweni, 2024). However, only 32% of respondents in Mtsweni's (2024) study provided cybersecurity awareness training, and only 41% of the organisations monitor cyber threats daily. Recognising the threat context, van Niekerk (2017) warned that organisations cannot always respond effectively to increasing cyberattacks.

The need for a responsive cybersecurity process is highlighted by persistent cyber threats. However, currently, there is limited research on the structure of a cybersecurity process. A Google Scholar search for "cybersecurity process" in the title yielded no matches. Prior studies have focused more on identifying strategies for effective cybersecurity management in organisations (Cheng & Wang, 2022; Ciekanowski *et al*. 2024). Or on strategies to manage cybersecurity behavioural risks (van Steen, 2025). Cybersecurity strategies see strategies can be viewed as variables independent of each other (Cloutier & Langley, 2020). Given the evolving cyber threat landscape, this study contributes to the literature by applying a process focus. Cloutier and Langley (2020) recommend considering process driven research in contrast to variable driven research to contribute to the literature.

To address this gap, this study models an organisation's strategic cybersecurity process using interviews with knowledgeable people from various areas, from information systems to internal audits. Understanding this process can assist managers in developing a more responsive

process in light of persistent and evolving cyber threats. Not only can modelling the process provide insight into which elements are key in the process, but the research can also assist managers in modelling their own processes that best fit their specific business context. This study follows a novel approach in South Africa by examining the strategic process used in a well-resourced organisation, by extending the research on cybersecurity initiated by Rajan *et al.* (2021) to a South African organisation. To model the process, this study used interpretive structural modelling (ISM). Although ISM is an established method, it is one of the underutilised research methods that is ideal for modelling a process. This has managerial implications, as managers can use ISM to model a process. In addition, strategic processes are contingent on the situation, specific to each organisation (Well & Olson, 1989). As such, this study contributes to the literature by using ISM to model the cybersecurity process in a well-resourced, sophisticated organisation in the South African financial sector by identifying the interrelationships between strategic cybersecurity elements.

This study aimed to identify the interrelationships between strategic cybersecurity management elements by interviewing specialists to model the underlying strategic cybersecurity process based on seven elements adapted from Rajan *et al*. (2021), in line with the ISM guidance provided by Singh and Kant (2008). By using the elements of a prior study, this study emphasises the need for organisations to model their own processes, as a single solution is unlikely given the different organisational contexts. Modelling each organisation's unique process can lead to improved insight into the applied cybersecurity process and highlight essential informal elements. A prior cybersecurity awareness study found different levels of cybersecurity awareness among students at different universities (Yildirim & Erendor, 2024). Interestingly, cybersecurity governance was found to be a dependent element in this study, whereas Rajan *et al*. (2021) found governance to be a driving element, highlighting the need for context-specific modelling. Whether cybersecurity governance is a driving power or contingent on factors such as the existing technology infrastructure and internal resources and capabilities can also depend on the information systems maturity of the organisation. The elements this study focuses on are summarised in Table 1.

Table 1: Cybersecurity elements

Element	Sources
Cybersecurity governance	(Maleh *et al.*, 2021; Rajan *et al.*, 2021)
Collaboration among departments	(Rajan *et al.*, 2021; Popoola, *et al.*, 2024)
Training and awareness	(Rajan *et al.*, 2021; Zwilling *et al.*, 2022)
Resources and capabilities	(Saunila *et al.*, 2019; Rajan *et al.*, 2021; Malatji *et al.*, 2022)

Information flow	(Patrick *et al.*, 2016; Rajan *et al.*, 2021)
Technological infrastructure	(Jayalath & Premaratne, 2021; Rajan *et al.*, 2021)
Third-party security risk	(Li & Xu, 2021)

This study models the cybersecurity strategic management process using interview inputs from cybersecurity experts and then assesses the interrelationships between the seven elements using ISM.

ISM is a technique used to establish interrelationships among elements using experts' knowledge of the elements' contexts (Farris & Sage, 1975). Expert knowledge is used to accommodate organisational-specific aspects, in line with the contingency theory's explanations of the optimisation of processes. Since ISM's formalisation and development by Warfield (1974), it has become an entrenched and trusted research method that can readily identify interrelationships in a process. The case in this study is an established, well-resourced organisation in the financial sector; its IT system comprises legacy and state-of-the-art systems. The participants were experts in cybersecurity-related matters and were drawn from a variety of functions within the organisation, ranging from information security to internal auditing.

The remainder of this paper is organised as follows. Section 2 reviews the literature on the key elements of cybersecurity. Section 3 describes the ISM method. The results are discussed in Section 4, followed by the conclusion in Section 5, which also highlights areas for further research.

2. LITERATURE REVIEW

The literature review begins by describing cybersecurity against cybersecurity risks. Thereafter, more information on the seven cybersecurity elements is included to contextualise the study.

2.1 Cybersecurity and cybersecurity risks

Cybersecurity (as a principle) is expected to protect an organisation's data and IT assets from security threats and vulnerabilities (Pieterse, 2021). However, the successful implementation and maintenance of cybersecurity protocols in organisations remains a challenge (van Niekerk, 2017). This challenge can be mitigated by implementing an adaptive, responsive strategy, as cyberattacks are also adaptive and are evolving to more easily produce and execute criminal actions (Falowo *et al.*, 2024). Advanced persistent threats (APTs) remain a challenge, especially in the current environment of rapid adoption of cloud computing, artificial

intelligence (AI), and machine learning (Kaspersky, 2024). A sinister aspect of this environment is the dark web, home to activities that result in a diversity of malicious AI bots, such as FraudGPT and WormGPT, which can be used to create spear-phishing emails and hacking tools (Khawaja, 2023) in record time.

Over and above technology's vulnerabilities, individuals still remain the main gateway for security breaches, and these may be malicious acts or the result of negligence or ignorance (Kempen, 2020). Insider threats are a major risk to organisations, as disgruntled employees with knowledge and access can easily act in malice or for personal gain (van Niekerk, 2017). Furthermore, criminal access to the organisation's systems is mainly gained via phishing attacks, where human vulnerabilities are exploited (Irwin & Dawson, 2019), using social engineering techniques (Kulkarni & Nath, 2024).

In addition, there is an increase in the security risks associated with third-party interactions and external service providers (Fischer, 2016). Third-party cyberattacks (also referred to as supply chain attacks) occur when hackers attack vendors or suppliers who have been granted access to the client organisation's network, code, software, or hardware (Madnick, 2022). An example is the SolarWinds attack in 2020, where an estimated 18 000 SolarWinds customers (from Fortune 1000 companies to government agencies) were affected (Graham, 2024).

To address evolving cyber threats, organisations are encouraged to increase their operational resilience by using strategic cybersecurity management to protect digital assets (Mughal, 2018). Modelling the strategic management process, particularly in light of the interrelationships between strategic cybersecurity elements, can improve responsiveness and resilience. This study adapted the seven critical cybersecurity elements identified by Rajan *et al*. (2021) and added third-party risks to the process while merging the security awareness and training elements into a single element. In addition, as the governance element in Rajan *et. al*. (2021) discusses aspects linked to cyber-attacks and security; this study used the term cybersecurity governance to differentiate the study from corporate governance. As a result, this study focused on the interrelationships between technological infrastructure, resources and capabilities, cybersecurity governance, collaboration among departments, secured information flow, management of third-party risk, cybersecurity training, and awareness as key elements for security management. These seven elements are listed in Table 1. A literature review that focuses on each of these seven elements is presented below.

2.2 Cybersecurity governance

In essence, cybersecurity governance integrates the elements of cyber defence with those of risk management (Maleh *et al.,* 2021). Cybersecurity governance provides the strategic vision

of how an organisation controls information assets within its risk appetite, and onto this it builds accountability and establishes decision-making responsibilities (PwC, 2017).

Within governance, four pillars of cybersecurity accountability have been identified: preparation, prevention, detection, and response (Singh, 2023). Preparation includes establishing cybersecurity policies, preparing and updating risk assessments, maintaining threat protection and intrusion detection processes, and updating business continuity plans and event responses (Mughal, 2018). The second pillar, data protection, addresses efforts to prevent the misuse of data and includes measures such as ensuring key infrastructure security, updated data loss prevention (DLP) protocols, data encryption, endpoint security, and training end-users (Perwej *et al.,* 2021).

The third pillar, detection, includes real-time security analysis, content identification, cyber-intelligence gathering, and cyber surveillance of all online traffic and network systems (Dlamini & Mbambo, 2019). The fourth pillar, response, includes the business continuity plan (BCP), which is integrated with an incident response plan (IRP). These ensure the continuous provision of essential services and enable quick recovery from the effects of cyberattacks (Mughal, 2018). An IRP outlines/allocates the responsibilities and processes to be followed to detect, respond to, and recover from cyber incidents (NIST, 2024) within the constraints of the organisation's resources and capabilities.

2.3 Resources and capabilities

Resources refer to the people, technology, and information assets of the organisation that enable it to implement strategies to improve system efficiency and effectiveness (Saunila *et al.*, 2019). Technology assets include data, infrastructure, firewalls, software, hardware, networks, cloud devices, data storage, and IT equipment for storing sensitive data (NIST, 2024). Organisations conduct threat analyses to determine critical IT assets or resources vulnerable to cyberattacks and then build adequate/appropriate security measures and prioritise resources (Razikin & Soewito, 2022). Without regular threat analysis, organisations' security measures may prove to be ineffective and fail to prevent or detect cyberattacks, leaving them vulnerable to security breaches (Perwej *et al.*, 2021). To minimise vulnerabilities, organisations typically use security configurations such as routers and wireless access points, disable excessive/surplus services, deploy robust validation protocols, and implement access control lists (Mughal, 2018).

The responsibility of the IT system is to support the organisation's information flow and maintain its ability to predict and manage any cyberattack or cyber infrastructure failure (Malatji *et al.*, 2022). The skills and infrastructure needed to detect incidents must be defined, regularly

tested, and approved by those with an overall responsibility for governance (NIST, 2024). Cybersecurity resources are mandated to detect unauthorised devices on the network, malicious software, and threats at all network perimeters, increasingly using machine learning to identify and adapt to counter new threats (Bharadiya, 2023). The adoption of machine learning is essential, as it has the ability to positively influence information flow.

2.4 Information flow

Information flow in the context of cybersecurity is a strategic organisational activity that ensures the communication of details of incidents and security decisions, thus creating awareness and improving security coordination (Patrick *et al.*, 2016). Shared information can include the results of regular vulnerability scanning to detect weaknesses in an application's code or configuration (Mughal, 2018). It can also include details of vulnerabilities that, if not addressed, can reduce information flow.

Information about and knowledge of security incidents, breaches, and vulnerabilities should influence the cybersecurity information strategy of an organisation and promote awareness (a key element of prevention) (Patrick *et al.*, 2016). Training is one of the best methods for creating awareness among employees regarding cybersecurity issues (Popoola *et al.*, 2024).

2.5 Cybersecurity training and awareness

Training helps create rational awareness of cybersecurity threats and countermeasures (Rama & Keevy, 2022). Such staff training and awareness creation measures are essential, as cybercriminals target individuals, manipulating their human susceptibility to trigger errors of judgment and exploiting any lack of technical knowledge and psychological weakness (Mcanyana *et al*., 2020). Cybersecurity training and awareness programs are intended to educate and train employees about cyberattack methods and prepare them on how best to respond by studying emergency scenarios and role play (Li *et al*., 2019).

The security culture of organisations, and particularly employees' security awareness, are essential aspects of the organisation's preparedness and resilience profile. This focus has become necessary because of the increasing frequency, intensity, and sophistication of cyber risks, especially as they increasingly target the human element (Andronache, 2021). Zwilling *et al.* (2022) highlighted the value of training, as better cyber knowledge improves cyber awareness, and in turn, awareness is associated with more effective use of protection tools. However, no amount of training can ultimately address an individual's preparedness to disclose information. This highlights the need for further research. Due to human weaknesses, even the most advanced technological security cannot protect an organisation from cyberattacks if the cybersecurity culture of the organisation does not encourage employees to

be careful and fully aware of their own weaknesses (Huang & Pearlson, 2019). In other words, better threat awareness, especially of new threats, is achieved through collaboration and information sharing (von Solms & van Niekerk, 2013).

2.6 Collaboration among departments

The objective of collaborative security is to share reliable information among employees to improve cybersecurity awareness (Ključnikov *et al*., 2019). Such collaboration can support a continuous learning culture and thus improve digital resilience (Popoola *et al.*, 2024). Information security collaboration assists in collecting, integrating, classifying, distributing, and sharing information, security knowledge, and threats. The process is essentially a dialogue between the organisation's IT experts and its employees (Safa *et al*., 2016); as such, it is an informal process.

Collaboration can assist in developing and sharing protection skills, threat detection techniques, and mitigation strategies (Guarascio *et al*., 2022). Employees' knowledge of potential cyber risks can decrease the number of security incidents resulting from human error or negligence (Mughal, 2018). Knowledge sharing not only improves an organisation's cybersecurity, it also helps create trust among employees (Pham *et al*., 2021), and thus improves the organisation's collective cyber intelligence. Cyber intelligence requires timely and reliable information sharing between employees and cybersecurity experts as trusted associates (Saeed *et a*l., 2023). The state of technological infrastructure can facilitate such collaboration through improved information flow.

2.7 Technological infrastructure

Technological infrastructure refers to computers, databases, servers, networks, and data platform capabilities that enable an organisation to build and run business applications; they are also used to manage the risk of cyberattacks (Accenture, 2023). Adequate and appropriate technological infrastructure ensures that organisations are able to build security capacity while maintaining uninterrupted services to customers (Jayalath & Premaratne, 2021). The key aspect of being able to provide uninterrupted services is the ability to withstand cyberattacks: this is achieved by using a well-built technological infrastructure that supports a solid internal cybersecurity process (Jayalath & Premaratne, 2021).

Organisations typically implement technological solutions, such as firewalls, intrusion prevention, data leakage prevention (DLP), network access control (NAC), and privileged access management (PAM) to support the information security landscape (Melaku, 2023). Data leakage prevention (DLP) uses antivirus software, AI, and machine learning to identify and avert unlawful distribution and removal of data and sensitive data leakage (Microsoft,

2024). Network access control (NAC) denies access to non-compliant devices and prevents unsecured nodes from infecting the network (Mughal, 2018). Privileged access management (PAM) is an identity security solution that monitors privileged access, detects and prevents unauthorised access to critical resources (Gartner, 2024).

However, despite the use of these techniques and technological solutions, it is imperative to continuously monitor the development of cyberthreats, such as malware, phishing attacks, ransomware, and associated social engineering attacks (Pawar & Palivela, 2022). A frequent review of technological infrastructure helps ensure that it can defend the system (Rai *et al*., 2020). Optimisation of the technological infrastructure can be achieved by implementing cybersecurity solutions aligned with the organisation's technology infrastructure strategy. This requires a clear understanding of the potential cybersecurity risks and abilities of the cybersecurity technology employed (Perwej *et al.*, 2021). Strategic cybersecurity solutions must provide end-to-end security: this must address technology, human participation, and protection of data applications (Thomas & Sule, 2023). Given the complexity and dynamism of the cyber world, cybersecurity can only be achieved if it extends collaboration to trusted outside entities, but this still increases the risk (Abrahams *et al*., 2024).

2.8 Third-party security risk

External sources within the organisation's cybersecurity ecosystem include suppliers, service providers, vendors, contractors, and partners, all with greater or lesser access to sensitive customer data, which poses third-party risk (Nevidita, 2023). Even if an organisation has an adequate cybersecurity system, its data is still vulnerable to third-party security risks (Keskin *et al*., 2021), as the use of third parties in the system is commonplace.

Cybercriminals gain unauthorised access by exploiting third parties' access to an organisation's corporate network, codes, software, or hardware to carry out data theft and disruption of business operations (Bhattacherjee, 2023). These attacks are particularly problematic when third-party suppliers have weaker security protocols, as they provide pathways for hackers to bypass the target organisation's security, no matter how strong it may be (Madnick, 2022). The majority of security breaches originate from vulnerabilities related to third parties (Keskin *et al*., 2021), and globally, 75% of breaches are attributed to third-party access. Such breaches result in service interruptions, ransomware attacks, and data breaches (Bhattacherjee, 2023).

Keskin *et al*. (2021) observed that organisations normally suffer security incidents due to inadequately managed third-party security risks. Almost every organisation relies on software created or managed by third parties, and any software is susceptible to vulnerabilities in its

code that can be exploited by hackers (Madnick, 2022). For example, if a company offers cloud services, its customers' data is at risk of hackers exploiting vulnerabilities in the cloud services provider's code or in the software on which the cloud service company relies (Madnick, 2022). As third-party data breaches become more common, organisations are encouraged to manage the security risks associated with third-party vendors with greater collaboration and oversight (Nevidita, 2023).

2.9 Literature overview

The above discussion highlights the complexity of cybersecurity by describing seven strategic cybersecurity elements. However, the relationship between technological infrastructure, resources and capabilities, cybersecurity governance, collaboration among departments, secured information flow, management of third-party risk, training, and awareness of cybersecurity is unclear. Thus, further research is needed to contextualise these elements in a strategic process.

3. METHODOLOGY

This study analyses the relationship between cybersecurity elements to model the strategic cybersecurity management processes. This study used interviews with ISM to analyse the interrelationships between the seven cybersecurity elements. The ISM methodology assists with the logical arrangement of the complex elements of a system (Farris & Sage, 1975). This method's interpretive nature allows participants to decide whether and, if so, to what extent the elements are related (Singh & Kant, 2008).

ISM modelling is structured using pairwise relationships between elements, with the overall process extracting insights on the inter-relationships between a complex set of elements to identify the underlying process (Rajan *et al*., 2021). Specific relationships and their overall structure are portrayed in a graphical model, as the direct and indirect relationships between elements describe the relationship better than individual elements in isolation (Singh & Kant, 2008). The ISM steps described in Table 2 provide insights into the collective associations between the strategic cybersecurity elements.

Table 2: Steps involved in the ISM technique

Steps	Description
Step 1. Identification of elements	This step involves identifying the elements that affect cybersecurity management within organisations.

Step 2: Developing a structural self-interaction matrix (SSIM)	Determine the relationships between each pair of elements established Step 1.
Step 3: Developing reachability matrix (RM) from the SSIM	The SSIM is converted into a binary matrix, called the RM.
Step 4: Partitioning the RM into different levels	Based established RM, elements are categorised into different levels using the antecedence relationships between them.
Step 5: ISM-based model	The process flow is then developed based on the established level of each element.
Source: Singh and Kant (2008:141-150).	

3.1 Step 1: Identification of elements

This step involves identifying the elements that affect cybersecurity management. These were based on the seven cybersecurity elements from Rajan *et al.* (2021) and were adapted by merging security awareness and training into one element, adding third-party risks as a separate element. This study used the term cybersecurity governance to differentiate the type of governance from corporate governance (refer to Table 1, which provides a summary of the elements and the literature review discussion in Section 2).

3.2 Step 2: Structural self-interaction matrix (SSIM)

To develop an SSIM, cybersecurity experts from a financial sector organisation in South Africa were interviewed to establish relationships between the seven cybersecurity elements identified from the literature. Nine anonymised cybersecurity experts were sampled from a population of 16 cybersecurity professionals using a purposive selection method. The criteria included accessible participants, cybersecurity qualifications, a minimum of five years in cybersecurity, a mix between junior and senior leadership roles, and different industry exposure. Semi-structured interviews were conducted to identify the relationship between cybersecurity elements and develop a strategic cybersecurity process flow.

The interview results were transcribed into a Microsoft Excel™ spreadsheet to facilitate further analysis of the interviewees' responses on the pair-wise relationship between the two elements. To analyse the results of the SSIM, the letters V, A, X, or O in cell (i; j) were noted; these were based on consensus answers using the process described by Singh and Kant (2008). Consensus answers mean that all respondents agreed on the pairwise relationship between two elements. The results in Table 3 indicate the relationship linking element number

(i) in the line of the cell with element number (j) in the column. These letters can be understood as follows:

- V – i reaches j, but j does not reach i.
- A – j reaches i, but i does not reach j.
- X – i reaches j, and j reaches i.
- O – i does not reach j, and j does not reach i.

Table 3: Structural self-interaction matrix (SSIM)

	Cybersecurity elements	7	6	5	4	3	2
1	Cybersecurity governance	X	A	A	X	A	O
2	Collaboration among departments	O	X	A	X	X	
3	Training and awareness	O	X	O	X		
4	Resources and capabilities	V	X	V			
5	Information flow	A	X				
6	Technological infrastructure	V					
7	Third-party security risk						

Thus, to allocate an X, all the respondents noted, for example, that element 1 reached to element 7, and that element 7 reached to element 1. Whereas an example of allocating A means that element 6 reached to element 1, but element 1 do not reach to element 6. O means the respondents did not agree that the elements reached to each other, while an example of allocating V means element 4 reached to element 7, but element 7 did not reach to element 4.

3.3 Step 3: Reachability matrix (RM)

The SSIM was converted into a binary matrix called the reachability matrix (refer to Table 4). During the conversion process, V, A, X, and O were substituted with 1 and 0. The substitutions help identify the driving or dependence power. The ”driving power for each barrier is the total number of [elements] (including itself), which it may help achieve, while the dependence power is the total number of [elements] (including itself), which may help achieve it” (Singh & Kant, 2008:146).

The substitution of 1s and 0s was based on the following rules described by Singh and Kant (2008):

V – the (i, j) entry in RM becomes 1 and the (j, i) entry becomes 0.

A – the (i, j) entry in RM becomes 0 and the (j, i) entry becomes 1.

X – the (i, j) entry in RM becomes 1 and the (j, i) entry also becomes 1.

O – the (i, j) entry in RM becomes 0 and the (j, i) entry also becomes 0.

Table 4: Reachability Matrix (RM)

	Cybersecurity elements	1	2	3	4	5	6	7	Driving power
1	Cybersecurity governance	1	0	0	1	0	0	1	3
2	Collaboration among departments	0	1	1	1	0	1	0	4
3	Training and awareness	1	1	1	1	0	1	0	5
4	Resources and capabilities	1	1	1	1	1	1	1	7
5	Information flow	1	1	0	0	1	1	0	4
6	Technological infrastructure	1	1	1	1	1	1	1	7
7	Third-party security risk	1	0	0	0	1	0	1	3
	Dependence power	6	5	4	5	4	5	4	

The RM shows high levels of interrelationships, and as the response time in the process could limit the responsiveness, the transitive links were not used in further analysis. However, transitive links were found between all the unconnected elements. Thus, an area of future research is to consider the timing in the process to optimise the strategic cybersecurity process. The dependence power (antecedence) and driving power (reachability) of the RM inform the level partitioning in Step 4.

3.4 Step 4: Level partitioning of elements

The reachability (driving power) and antecedent (dependence power) sets for each element were identified from the RM, as recommended by Warfield (1974). The reachability set consists of row elements representing the driving power. The reachability set shows the element itself and other elements which it may reach, whereas the antecedent set consists of the element itself and other elements which may reach it (Mandal & Deshmukh, 1994). The antecedent set consisted of column elements or dependence power, whereas the intersection set consisted of common elements in the reachability and antecedent sets to identify the levels of partitioning, as noted in Table 5. The levels are identified when the reachability set matches the intersection set using an interactive process. For example, as the reachability sets for elements 1and 2 are the same as the intersection sets, elements 1 and 2 are on level I. For the next iteration, elements 1 and 2 are excluded throughout to identify level II. After elements 1 and 2 are excluded from the sets, the intersection of elements 3 and 5 is the same as the reachability, making them level II elements. The interactive process excludes elements linked

to levels already identified in an iterative process to determine the next level until all levels are identified.

Table 5: Level partitioning of elements

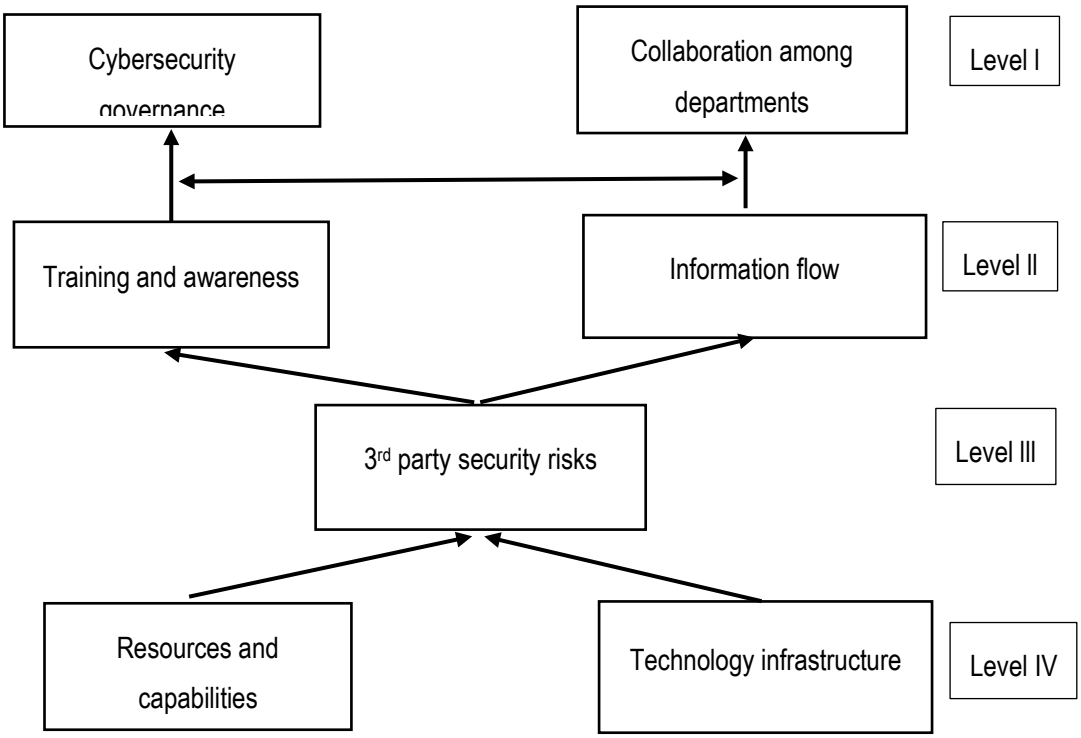
Element no	Reachability set	Antecedent set	Intersection set	Level
1	1, 4, 7	1, 3, 4, 5, 6, 7	1, 4, 7	I
2	2, 3, 4, 6	2, 3, 4, 5, 6	2, 3, 4, 6	I
3	1, 2, 3, 4, 6	2, 3, 4, 6	2, 3, 4, 6	II
4	1, 2, 3, 4, 5, 6, 7	1, 2, 3, 4, 6	1, 2, 3, 4, 6	IV
5	1, 2, 5, 6	4, 5, 6, 7	5, 6	II
6	1, 2, 3, 4, 5, 6, 7	2, 3, 4, 5, 6	2, 3, 4, 5, 6	IV
7	1, 5, 7	1, 4, 6, 7	1, 7	III

3.5 Step 5: ISM-based model – process flow

Based on the results of level partitioning, the process flow presented in Figure 1 was developed, showing the levels of cybersecurity elements. In today's rapidly evolving technological landscape, organisations face numerous cybersecurity challenges (Mughal, 2018). Cyberattacks are among the fastest-growing crimes and are becoming increasingly sophisticated, making it crucial for organisations to implement responsive cybersecurity approaches to safeguard their data and information (Yusif & Hafeez-Baig, 2021).

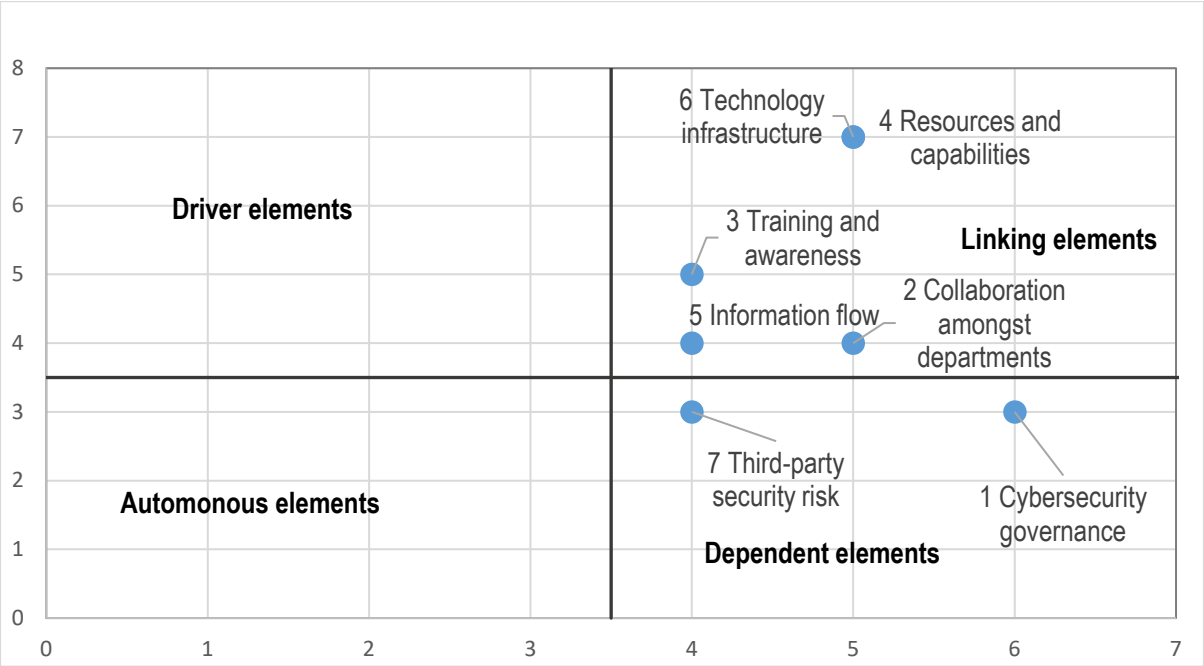
The process flow presented in Figure 1 was developed based on the results of the level partitioning from the ISM process, showing resource capabilities and technology infrastructure as the basis of the process in level IV, while level I, with cybersecurity and collaboration among departments, is the outcome. The more fixed nature of resources and capabilities, technology infrastructure (level IV), and third-party risks (level III) seems applicable to a foundation. In contrast, training, awareness, and information flow (level II) with collaboration between departments (level I) need to be more adaptive or responsive. Surprisingly, cybersecurity governance is not a driving element but a dependent element.

Figure 1: ISM process flow



To position the driving, linking, autonomous, and dependence power of the elements, a MICMAC analysis is shown in Figure 2. The MICMAC figure comprises quadrants that represent the driver or independent elements, autonomous elements, linking elements, and dependent elements. Given the interactive relationship between the cybersecurity strategic elements, there are five linking elements. They are technology infrastructure, resources and capabilities, training and awareness, information flow, and collaboration among departments. There are two dependent elements: third-party security risks and cybersecurity governance. Surprisingly, there are no driver or autonomous elements, possibly because of the sophistication of the case. These results differ from those of Rajan *et.al*. (2021), who found governance to be linked to cybersecurity to be a driver. The differences show the need for responsive processes, as there is no single solution, and every organisation's strategic process will be contingent on the environment it is in (Well & Olson, 1989). The iterative nature is evident in the number of linking elements, where both the driving and dependent powers are high. Even though the technology infrastructure and resources and capabilities have high driving powers, their dependent powers are also strong.

Figure 2: MICMAC analysis of the cybersecurity elements



4. FINDINGS AND DISCUSSION

This study modelled the cybersecurity strategic management process using interview inputs from cybersecurity experts to assess the interrelationships between the seven elements using ISM. Given the interactive relationship between the cybersecurity strategic elements, there are five linking elements. They are technology infrastructure, resources and capabilities, training and awareness, information flow and collaboration among departments. It has two dependent variables: third-party security risk and cybersecurity governance. There were no driver or autonomous elements. The iterative nature is evident in the number of linking elements, where both the driving and dependent power are high. Even though the technology infrastructure and resources and capabilities have high driving powers, their dependent powers are also strong.

The most obvious limitation of this study is that it used specialist respondents in a case study. Even though specialists were used, their views could have been influenced by their experiences. In addition, a focus on one case limits the generalisability of the results. However, as strategic processes are in essence designed to develop competitive advantages, using the research method applied in this study to identify strategic cybersecurity factors and the underlying process used can help managers refine the process in their organisations. Despite the limitations, this study does extend the research on strategic cybersecurity management conducted by Rajan *et al*. (2021) to a South African organisation.

One element that this study did not consider is time. As such, future research could consider the response times between the elements. It would be especially useful to understand aspects of the time lag in communication between departments when reporting cybersecurity concerns and the initiation of remedial responses. Further research should consider other emerging cybersecurity issues. Artificial intelligence (or AI), for example, is both a powerful tool for achieving a secure cyber environment, and for breaching the defences entities install to protect their businesses.

5. MANAGERIAL IMPLICATIONS

Modelling a cybersecurity process has managerial implications as a process in which the key elements interact is more visible. Managers can use the ISM process to model their own unique strategic processes, especially as strategic processes are bound to keep evolving to adapt to the fast pace of change brought about by Industry 4.0. The model also shows the value of linking informal elements with formal elements in a process. However, an area of future research is to also consider how fast the process works, or whether there are time delays between elements that could make the process ineffective. Researching the changes in the processes over time can also shed light on how the elements change or change position in the process over time to show whether or not the process evolves. In addition, a well-resourced and mature company might follow a different process, given an established level of infrastructure and responses in comparison to a new company.

6. CONCLUSION

The purpose of this study was to assess the relationship between cybersecurity elements and to uncover the linked cybersecurity process. Primary data were collected from nine anonymised cybersecurity experts in South Africa, using a case study design. Semi-structured interviews were used with the intention of establishing the relationship between seven cybersecurity elements (identified in the literature review), using the interpretive structural method (ISM) to develop a cybersecurity process flow.

ISM results showed that all cybersecurity elements were interrelated. A cybersecurity-element process flow was developed using the ISM methodology with a MICMAC analysis. The process starts with technology infrastructure, resources and capabilities on level IV, with third-party security on level III. This is followed (in level II) by training, awareness and information flow. Collaboration among departments and cybersecurity governance were the outcomes of the process, which were placed at level I.

The iterative nature of the relationships between strategic cybersecurity elements is evident in that five of the seven elements are linking elements, with third-party security risks and cybersecurity governance as dependent elements. Further research on the timeframe implicit in the process, as well as other strategic cybersecurity elements, can enrich the understanding of the use of a strategic cybersecurity process in a business environment. Other future research options include using focus groups to identify especially informal cybersecurity elements that could be a key component to enable a resilient process that can respond in a timely manner to threats. Additional insights can be gained using a more longitudinal study to see if the process changes over time, possibly in response to changes in technologies and cyber threats. Considering a cross-sectional study in the same sector as a form of benchmarking can isolate different practices between companies, which can lead to further improvements in the strategic cybersecurity process. Additional considerations, in the use of informal elements to enhance the process, can help improve the process as well as the speed at which the process informs improvements in the entire strategic cybersecurity process.

Conflict of interest: The authors declare no conflict of interest with respect to the research, authorship, and publication of the article.

Data availability: The data used for this article are available upon request from the authors.

Ethical clearance and informed consent statement: The researchers obtained ethical clearance from the University of Pretoria (EMS138/23) prior to data collection and obtained informed consent from all participants in this study.

Funding: The authors did not receive any financial support for research, authorship, and publication of the article.

REFERENCES

Abrahams, T.O., Farayola, O.A., Kaggwa, S., Uwaoma, P.U., Hassan, A.O. & Dawodu, S.O. (2024). Cybersecurity awareness and education programs: A review of employee engagement and accountability. *Computer Science & IT Research Journal, 5*(1), 100-119. https://doi.org/10.51594/csitrj.v5i1.708

Accenture. (2023). *IT infrastructure*. https://www.accenture.com/cz-en/insights/cloud/it-infrastructure-index

Andronache, A. (2021). Increasing security awareness through lenses of cybersecurity culture. *Journal of Information Systems & Operations Management*, *15*(1), 7-22.

Bharadiya J. (2023). Machine learning in cybersecurity: Techniques and challenges. *European Journal of Technology*, *7*(2), 1-4. https://doi.org/10.47672/ejt.1486

Bhattacherjee, S. (2023). *Third-party cyber risk: Understanding the cyber threat landscape of third parties*. https://signalx.ai/blog/third-party-cyber-risk/

Cheng ECK, Wang T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information*, *13*(4), 1-14. https://doi.org/10.3390/info13040192

Ciekanowski, M., Żurawski, S., Pauliuchuk, Y., Ciekanowski, Z. & Marciniak, S. (2024). Strategies for effective cybersecurity management in organizations. *European Research Studies Journal*, *27*(1), 365-379.

Cloutier, C. & Langley, A. (2020). What makes a process theoretical contribution? *Organization Theory*, *1*(1), 1-30. https://doi.org/10.1177/2631787720902473

Dlamini, S. & Mbambo, C. (2019). Understanding policing of cybercrime in South Africa: The phenomena, challenges and effective responses. *Cogent Social Sciences*, *5*(1), 1-13. [https://doi.org/10.1080/23311886.2019.1675404].

Falowo, O.I., Ozer, M., Li, C. & Abdo, J.B. (2024). Evolving malware & ddos attacks: Decadal longitudinal study. *IEEE Access*, *12*, 39221-39237.

Farris, D.R. & Sage, A.P. (1975). On the use of interpretive structural modeling for worth assessment. *Computers & Electrical Engineering, 2*(2-3), 149-174. https://doi.org/10.1016/0045-7906(75)90004-X

Fischer, E. (2016). *Cybersecurity issues and challenges: In brief.* https://sgp.fas.org/crs/misc/R43831.pdf

Gartner. (2024). *What are privileged access management?* https://sgp.fas.org/crs/misc/R43831.pdf

Graham, K. (2024). *What is a third-party data breach? 5 recent examples*. https://www.bitsight.com/blog/third-party-data-breach

Guarascio, M., Cassavia, N., Pisani, F.S. & Manco, G. (2022). Boosting cyber-threat intelligence via collaborative intrusion detection. *Future Generation Computer Systems*, *135*, 30-43. https://doi.org/10.1016/j.future.2022.04.028

Huang, K. & Pearlson, K. (2019). *For what technology can't fix: Building a model of organizational cybersecurity culture*. Proceedings of the 52nd Hawaii International Conference on System Sciences https://doi.org/10.24251/HICSS.2019.769

Irwin, A.S. & Dawson, C. (2019). Following the cyber money trail: global challenges when investigating ransomware attacks and how regulation can help. *Journal of Money Laundering Control, 22*(1), 110-131. https://doi.org/10.24251/HICSS.2019.769

Jayalath, J. & Premaratne, S. (2021). Analysis of key digital technology infrastructure and cyber security consideration factors for fintech companies. *International Journal of Research Publications, 84*(1), 128-135. https://doi.org/10.47119/IJRP100841920212246

Kaspersky. (2024). *What is APT (Advanced Persistent Threat)?* https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

Kempen, A. (2020). Expert's view on: The growing cyber risk emanating from within. *Servamus Community-based Safety and Security Magazine, 113*(6), 54-55. https://hdl.handle.net/10520/EJC-1dbe79028e

Keskin, O.F., Caramancion, K.M., Tatar, I., Raza, O. & Tatar, U. (2021). Cyber third-party risk management: A comparison of non-intrusive risk scoring reports. *Electronics, 10*(10), 1168. https://doi.org/10.3390/electronics10101168

Khawaja, R. (2023). *FraudGPT: the dark evolution of ChatGPT into an AI weapon for cybercriminals in 2023.* https://datasciencedojo.com/blog/fraudgpt/

Ključnikov, A., Mura, L. & Sklenár, D. (2019). Information security management in SMEs: factors of success. *Entrepreneurship and Sustainability Issues, 6*(4), 2081-2094. https://doi.org/10.9770/jesi.2019.6.4(37)

Kulkarni, A.V. & Nath, S. (2024). *Human susceptibility to social engineering attacks: an innovative approach to social change*. IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI) in Gwalior, India... https://doi.org/10.1109/IATMSI60426.2024.10502492

Li, L., He, W., Xu, L., Ash, I., Anwar, M. & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management,* 45(2019), 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Li, Y. & Xu, L. (2021). Cybersecurity investments in a two-echelon supply chain with third-party risk propagation. *International Journal of Production Research,* 59(4), 1216-1238. https://doi.org/10.1080/00207543.2020.1721591

Madnick, S. (2022). The rising threat to consumer data in the cloud. *Apple*. https://www.apple.com/newsroom/pdfs/The-Rising-Threat-to-Consumer-Data-in-the-Cloud.pdf

Malatji, M., Marnewick, A.L. & von Solms, S. (2022). Cybersecurity capabilities for critical infrastructure resilience. *Information & Computer Security, 30*(2), 255-279. https://doi.org/10.1108/ICS-06-2021-0091

Maleh, Y., Sahid, A. & Belaissaoui, M. (2021). A maturity framework for cybersecurity governance in organizations. *Electronic Data Processing Audit, Control, and Security Newsletter (EDPACS), 63*(6), 1-22. https://doi.org/10.1080/07366981.2020.1815354

Mandal, A. & Deshmukh, S. (1994). Vendor selection using interpretive structural modelling (ISM). *International Journal of Operations & Production Management, 14*(6), 52-59. https://doi.org/10.1108/01443579410062086

Matsepe, N.T. & van der Lingen, E. (2022). Determinants of emerging technologies adoption in the South African financial sector. *South African Journal of Business Management, 53*(1), 1-12. https://doi.org/10.4102/sajbm.v53i1.2493

Mcanyana, W., Brindley, C. & Seedat, Y. (2020). *Insight into the cyber threat landscape in South Africa*. https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa

Melaku, H.M. (2023). A dynamic and adaptive cybersecurity governance framework. *Journal of Cybersecurity and Privacy, 3*(3), 327-350. https://doi.org/10.3390/jcp3030017

Microsoft. (2024). *Data loss prevention defined*. https://www.microsoft.com/en-us/security/business/security-101/what-is-data-loss-prevention-dlp#:~:text=Data%20loss%20prevention%20is%20a,based%20locations%2C%20and%20endpoint%20devices

Mtsweni, J. (2024). *CSIR issues national survey results on the state of cybersecurity in South Africa*. https://www.csir.co.za/csir-issues-national-survey-results-on-state-cybersecurity-south-africa

Mughal, A.A. (2018). The art of cybersecurity: defense in depth strategy for robust protection. *International Journal of Intelligent Automation and Computing, 1*(1), 1-20.

Nevidita, J.P. (2023). *47 third party data breach statistics: the numbers you need to know*. https://www.getastra.com/blog/security-audit/third-party-data-breach-statistics/#:~:text=In%202022%2C%20it%20took%20an,company%20getting%20into%20the%20network

NIST. (2024). *NIST incident response plan: Process, lifecycle, and templates*. https://www.cynet.com/incident-response/nist-incident-response/

Patrick, H., van Niekerk, B. & Fields, Z. (2016). Security-information flow in the South African Public Sector. *Journal of Information Warfare, 15*(4), 68-85.

Pawar, S. & Palivela, D.H. (2022). LCCI: a framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Information Management Data Insights, 2*(1), 1-13. https://doi.org/10.1016/j.jjimei.2022.100080

Perwej, D.Y., Qamar Abbas, S., Pratap Dixit, J., Akhtar, D.N. & Kumar Jaiswal, A. (2021). A systematic literature review on the cyber security. *International Journal of Scientific Research and Management, 9*(12), 669-710. https://doi.org/10.18535/ijsrm/v9i12.ec04

Pham, H.C., Ulhaq, I., Nguyen, M. & Nkhoma, M. (2021). An exploratory study of the effects of knowledge sharing methods on cyber security practice. *Australasian Journal of Information Systems*, *25*, 1-25. https://doi.org/10.3127/ajis.v25i0.2177

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

Popoola, O.A., Akinsanya, M.O., Nzeako, G., Chukwurah, E.G. & Okeke, C.D. (2024). Exploring theoretical constructs of cybersecurity awareness and training programs: comparative analysis of African and US Initiatives. *International Journal of Applied Research in Social Sciences, 6*(5), 819-827. https://doi.org/10.51594/ijarss.v6i5.1104

PwC. 2017. *Governing cybersecurity risk: It's time to take it seriously*. https://www.pwc.co.uk/issues/cybersecurity-services/insights/governing-cybersecurity-risk.html

Rai, A., Singh, A.S. & Kumar, A.S. (2020). A review of information security: issues and techniques. *International Journal for Research in Applied Science & Engineering Technology, 8*(5), 953-960. https://doi.org/10.22214/ijaset.2020.5150

Rajan, R., Rana, N.P., Parameswar, N., Dhir, S., Sushil, Y.K. & Dwivedi, Y.K. (2021). Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management. *Technological Forecasting and Social Change, 170*(2021), 1-18. https://doi.org/10.1016/j.techfore.2021.120872

Rama, P. & Keevy, M. (2022). A comparative review of South Africa's government-led cybersecurity awareness measures to those of world-leading countries. *Southern African Journal of Accountability and Auditing Research, 24*(1), 117-128. https://doi.org/10.54483/sajaar.2022.24.1.8

Razikin, K. & Soewito, B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. *Egyptian Informatics Journal, 23*(3), 383-404. https://doi.org/10.1016/j.eij.2022.03.001

Saeed, S., Suayyid, S.A., Al-Ghamdi, M.S., Al-Muhaisen, H. and Almuhaideb, A.M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors*, *23*(16), 7273. https://doi.org/10.26740/vubeta.v2i2.36031

Safa, N.S., von Solms, R. & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*(2016), 70-82. [https://doi.org/10.1016/j.cose.2015.10.006

Saunila, M., Ukko, J. & Rantala, T. (2019). Value co-creation through digital service capabilities: The role of human factors. *Information Technology & People, 32*(3), 627-645. https://doi.org/10.1108/ITP-10-2016-0224

Savaş, S. & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review, 3*(1), 7-34. https://doi.org/10.1365/s43439-021-00045-4

Singh, M.D. & Kant, R. (2008). Knowledge management barriers: an interpretive structural modeling approach. *International Journal of Management Science and Engineering Management, 3*(2), 141-150. https://doi.org/10.1080/17509653.2008.10671042

Singh, S. (2023). *Accountability in cybersecurity: Save money, reduce cyber risk.* https://blogs.blackberry.com/en/2023/01/accountability-in-cybersecurity

Thomas, G. & Sule, M.J. (2023). A service lens on cybersecurity continuity and management for organizations' subsistence and growth. *Organizational Cybersecurity Journal: Practice, Process and People, 3*(1), 18-40. https://doi.org/10.1108/OCJ-09-2021-0025

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

van Steen, T. (2025). Developing a behavioural cybersecurity strategy: a five-step approach for organisations. *Computer Standards & Interfaces*, *92*(2025), 1-8. https://doi.org/10.1016/j.csi.2024.103939

von Solms, R. & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*(2013), 97-102. [https://doi.org/10.1016/j.cose.2013.04.004].

Warfield, J.N. (1974). Developing interconnection matrices in structural modeling. *IEEE Transactions on Systems, Man, and Cybernetics, 4*(1), 81-87. [https://doi.org/10.1109/TSMC.1974.5408524].

Well, P. & Olson, M.H. (1989). An assessment of the contingency theory of management information systems. *Management Information Systems*, *6*(1), 59-85. https://doi.org/10.1080/07421222.1989.11517849

Yildirim, M. & Erendor, M.E. (2024). A comparative analysis of cyber security behaviours of university students. *Electronic Data Processing Audit, Control, and Security Newsletter (EDPACS*), *69*(6), 28-45. https://doi.org/10.1080/07366981.2024.2356298

Yusif, S. & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. *Journal of Applied Security Research*, *16*(4), 490-513. https://doi.org/10.1080/19361610.2021.1918995

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F. & Basim, H.N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82-97. https://doi.org/10.1080/08874417.2020.1712269