Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management

Rishabh Rajan
Department of Management Studies
Indian Institute of Technology Delhi
New Delhi, India
Email: rishabh12345rajan@gmail.com

Nripendra P. Rana*
School of Management
University of Bradford
Richmond Road, BD7 1DP, Bradford, UK
Email: nrananp@gmail.com

Nakul Parameswar
Institute of Rural Management Anand (IRMA),
Post Box No. 60, Near NDDB, Anand 388001, Gujarat State, India
Email: nakul.parameswar@gmail.com

Sanjay Dhir
Department of Management Studies
Indian Institute of Technology Delhi
New Delhi, India
Email: sanjaydhir.iitd@gmail.com

Sushil
Department of Management Studies
Indian Institute of Technology Delhi
New Delhi, India
Email: profsushil@gmail.com

Yogesh K. Dwivedi
Emerging Markets Research Centre (EMaRC)
School of Management
Swansea University, Fabian Bay, Swansea, SA1 8EN, UK
Email: ykdwivedi@gmail.com

***Corresponding Author**

Abstract

Cybersecurity is a serious issue that many organizations face these days. Therefore, cybersecurity management is very important for any organization. Organizations should learn to deal with these cyber threats through effective management across all business functions. The main purpose of this study is to identify the factors that affect cybersecurity within an organization and analyze relationships among these factors. The modified total interpretive structural modeling (M-TISM) technique is used to build a hierarchical model and define the common interactions between the factors. This study presents the impact of collaboration, training, resources and capabilities, information flow, technology awareness, and technological infrastructure on effective cybersecurity management. In addition, the study also explains the interrelationships among the identified factors in the M-TISM model.

Keywords: Cybersecurity, Strategy, M-TISM, Modified total interpretive structural modeling

1. Introduction

Over the last few years, national and multinational organizations have seen high growth in the usage of information systems, networks, and technologies to share information and knowledge from organizations to various business units. Most organizational units use a networked process and Internet servers to allow other business clients to access real-time data and information across the points of the network (Subashini and Kavitha, 2011). At the same time, there has been an explosion in the use of servers, networks, and virtual space. Several organizations are suffering from cyber threats and vulnerabilities (Mukhopadhyay et al., 2019; Romanosky, 2016). The cyber risk environment has grown in coverage and complexity over the last few years. During recent years, many public and private sector organizations have made numerous efforts to guarantee cybersecurity within their organizations. Despite all these efforts, the issues of cybersecurity strategy and the approach toward implementing the cybersecurity strategy still persist within these various organizations and also other firms (Liao et al., 2017; Osho and Onoja, 2015; Von Solms and Van Niekerk, 2013).

Cybersecurity management can be defined as an organization's strategic-level capability to protect information technology (IT) systems, information resources, and digital processes in an emerging cyber threat environment (Ferdinand, 2015; Jenab and Moslehpour, 2016). Cybersecurity management helps the organization to protect the confidentiality, integrity, and availability of its information through legal, administrative, and managerial controls (Ferdinand, 2015). Any firms aiming to address their informational threats and cyber risks must navigate the large and complex landscape of cybersecurity management and organizational strategies (Gordon, Loeb, and Sohail, 2003; Ključnikov, Mura, and Sklenár 2019; Lee, 2020; Zafar, Ko,i and Osei-Bryson, 2016).

Exterior to organizations and firms, cyberspace criminals and malicious actors in IT always search relentlessly for vulnerabilities within the organizational information system and employ both socio-technical and communal exploits such as malware injections and phishing practices within the structure of IT management (Tetri and Vuorinen, 2013; Zhang et al., 2015). Cybersecurity management within the organization is an exceptionally complicated matter (White, 2016), and the implementation and functioning of security safeguards are merely a part of strategic management. Cybersecurity is a critical issue (Rothrock, Kaplan, and Van Der Oord, 2018; White, 2016) because of evolving cyber-attacks, network breaches, equipment failure, industrial spies, user errors, and cyber threats within organizations (Liu et al., 2012). Despite the fact that many organizations are increasing their security investments, cyber-attacks are on the rise across the world (Rothrock, Kaplan, and Van Der Oord, 2018). An organization is required to advance its strategy and management to ensure its cybersecurity requirements (Gordon, Loeb, and Sohail, 2003; Lee, 2020). Within this perspective, it is vital to look at strategic factors in cybersecurity management within organizations.

Several studies (Ahmad, Maynard, and Park, 2014; Blake, 2007; Chaudhry, Chaudhry, and Reese, 2012; Dawes, 2008) have examined the impact of e-governance, network security, information security, cybercrime, knowledge management (Wang and Wang, 2019), collaboration (Chen, Chong, and Zhang, 2004; Ključnikov, Mura, and Sklenár, 2019), and knowledge transfer (David, Keupp, and Mermoud, 2020) on cybersecurity management within organizations.

The role of security policy (Hagen, Albrechtsen, and Hovden, 2008; Knowles et al., 2015), security awareness (Chang and Yeh, 2006; Li et al., 2019), top management support (Ključnikov, Mura, and Sklenár, 2019; Ma, Schmidt, and Pearson, 2009), information security cultures (Knapp et al., 2006), and technological infrastructure (Dawson, 2018) on cybersecurity management have also been studied by many researchers. Surprisingly, there are still a limited number of works (Chaudhry, Chaudhry, and Reese, 2012; Lee, 2020; Chander, Jain, and Shankar, 2013) that show the interrelationships among these variables and their combined impact on cybersecurity management within organizations; but the importance of the hierarchical model of cybersecurity management and the interrelationships of these factors for cybersecurity management using M-TISM has been overlooked. There is a rich literature available on cybersecurity management (Chander, Jain, and Shankar, 2013; Ferdinand, 2015; Jenab and Moslehpour, 2016) but very little of it has attempted to develop a theoretical framework (Kortjan and Von Solms, 2014; Li et al., 2019) of the various factors available in the literature. Therefore, there is a need to identify and evaluate key factors using the M-TISM approach that can ensure cybersecurity management within the organization. Hence, it is necessary to bridge these gaps in the cybersecurity literature by identifying the critical factors, developing contextual relationships, and constructing a hierarchical theoretical framework of identified factors based on the literature review. Therefore, this study will try to address the following research questions (RQs):

RQ1. What are the critical factors that lead to cybersecurity management within organizations?

RQ2. What are the various interrelationships among these identified factors in the context of cybersecurity management?

RQ3. How can we line up these identified factors for effective cybersecurity management within organizations?

Cybersecurity management is an integral part of any organization. In the modern computerized environment, cybercrime and cyber-attack have become a vital threat for organizations. According to Cyber Security Report (2020), nearly 27 percent of all organizations worldwide have been affected by cyber-attacks involving electronic devices. A total of 43 percent of enterprises in the UK had experienced a cyber-attack, while 38 percent of small companies were unable to defend themselves from cybersecurity threats (Cyber Security Breaches Survey, 2018). The most frequent attacks were fraudulent emails, malware, and attempts to expose institutional passwords, financial information, etc. In the current COVID-19 pandemic, online platforms, computer networks, and technology are increasingly being used by organizations, private businesses, and government institutions. Organizations generate and store large quantities of customer data/information, details of credit cards, payment data, healthcare information, consumption data, etc. These have all increased the threats of cybercrime, resulting in major developments in the field of cybersecurity management.

Therefore, the critical factors contributing to cybersecurity management, different interrelationships between these factors, and a model for lining up these factors for successful cybersecurity management within organizations must be properly understood. There is a need to identify critical factors for cybersecurity management and examine the interrelationships within the organization in order to make clear and understandable decisions for managing the organization’s cybersecurity posture. This aim of this study is to identify and analyze the critical factors that can contribute to effective cybersecurity management within organizations. Hence, the key objectives of this study are (1) to identify the critical factors in cybersecurity management within organizations, (2) to explore interrelationships among identified factors in cybersecurity management, and (3) to develop a hierarchical model of the identified factors in cybersecurity management. This study contributes to the cybersecurity management literature by establishing a contextual relationship between the identified factors through a systematic methodology. This study contributes to the theory of information security by showing how knowledge and information can be developed and utilized for cybersecurity management through training (Berry and Berry, 2018) and collaboration (Safa et al., 2018). From the practitioner's viewpoint, this study describes a hierarchical structure of identified factors in the context of cybersecurity management within organizations. The hierarchical structure developed through the M-TISM technique would help managers to develop organizational strategies to improve their cybersecurity management processes within organizations.

The remaining sections of this study are structured as follows: A brief literature review on cybersecurity is presented in Section 2. The methodology for this study is described in Section 3. In Section 4, the results and discussion are presented. Section 5 includes theoretical contributions and implications. Next, Section 6 presents the theoretical model along with proposition and Section 7 discusses the limitations and future research. Finally, Section 8 concludes the study.

2. Literature Review

Cybersecurity issues are attracting more attention and is of interest across the world. Additionally, 50 nations have published various forms of documents and articles of strategy, outlining their official stance on cyberspace, cyberspace security and attacks, and information security and safety (Switzer and Wang, 2017). Cybersecurity is the technique of protecting Internet-connected networks, servers, computers, and information from unauthorized attacks to ensure security against cyber threats (Solms and Niekerk, 2013). Cyber threats and hazards begin from an external onslaught or from an internal source such as a dissatisfied employee (Bulgurcu et al., 2010) and compromise a PC database or network from within (Moore, 2010). These Internet or virtual attacks multiply more speedily than other crimes; they are also a reason for financial crackdowns, and they affect the marketing flow, trademark, and brand image of the breached unit. Several previous studies have noted the impact of cybersecurity lapses on businesses and firms (Abomhara, 2015; Campbell et al., 2003; Cavusoglu et al., 2004).

Organizations often struggle for information/data security, and severe harm is caused to their finances and reputation. Hence, a series of clearances are provided by many observers handling cyberspace security problems to guarantee the desired outcomes by developing policies and strategies for security awareness (Li et al., 2019; Wiley, McCormac, and Calic, 2020), training programs, and reward systems. Wider research on cybersecurity and management has focused on the foundation of hierarchy and appropriate behavior by employees and workers toward security concerns (Solms and Niekerk, 2013). The information and cybersecurity management culture are also a significant part of organizational culture (Leidner, 2010; Leidner and Kayworth, 2006; Schlienger and Teufel, 2003), which is mainly concerned with employees' perceptions (Hu et al., 2012; Ngo et al., 2005). To prevent security threats in cyberspace and to identify and manage risks, the coherence of network traffic checking or monitoring and the ability to act on planned and strategic analyses need to be enhanced (Franke and Brynielsson, 2014).

Numerous studies reveal that technology and tools are increasingly used to threaten, cause humiliation, express annoyance, and harassment, and wreak psychological damage as cyberbullying has grown to be the key concern for modern society (Franke and Brynielsson, 2014; Solms and Niekerk, 2013). Cyberbullying and attacks have become widely recognized as a threat to information security (Franke and Brynielsson, 2014; Ortega-Ruiz et al., 2012). Also, the entertainment industry is directly affected through the sharing of information systems and technology. A vast amount of revenue is lost as a consequence of illegal data, and digital media can also operate in such a way that it will be easier to carry out illegal actions in the future. Also, it directly affects the monetary well-being and safety of the legal and authorized proprietor of the rights to the particular media. A few studies (Bieda and Halawi, 2015;

Gilmour, 2014) have noted the prevalent use of IT and cyberspace by terrorist-type organizations. Cyberspace terrorism is defined as the use of the Internet to conduct violence and threaten and cause loss of life or significant harm for political gain (Farn et al., 2004). The protection and safety of such critical communications form a significant part of cyberspace security and strategic management (MOD, 2011).

Based on the literature review, we have identified seven factors (see Table 1) that influence cybersecurity management within organizations. The identified factors include resources and capabilities, information flow, training, alliance and collaboration, governance, security awareness, and the technological infrastructure of an organization. The identified factors were cross-checked by experts from academia and industry. These factors are discussed in various subsections below.

2.1 Resources and Capabilities

Resources are the collection of assets and stocks available to the organization that are used for production (Raphael and Schoemaker, 1993; Saunila et al., 2019), whereas capabilities are an organization's ability to set up resources using managerial processes and are often extended into functional and sub-functional categories by mixing human, physical, and technological assets (Grant, 1999; Sedera and Gable, 2010). Like all other technologies, cyberspace and its security have been profoundly influenced by organizational resources and capabilities (Mandal, 2019; Saunila et al., 2019). Previous studies confirm that the availability of resources and capacity and resource platforms leads organizations to choose cyber and information security management. The maximum level of information and cyberspace security management is determined by factors related to the quality of investment and is generally related to the current IT capabilities of an organization and the measures that each firm uses to access cyberspace security management and investment decisions (Ekelund and Iskoujina, 2019).

2.2 Information Flow

The information includes usable data and records and contains estimates from data or data details (Ackoff, 1989). The flow of knowledge and information, particularly, supports security interactions without relying on access control models or trusted entities that underlie the security of a system, and has the task of ensuring the best possible use of information for achieving cybersecurity goals (Akella et al., 2010; Dhir and Sushil, 2017; Gonçalves et al., 2016; Sousa and González-Loureiro, 2016). Information flows through written, verbal, or electronic means within firms and organizations (Yazici, 2002; Zammuto et al., 2007), to a receiver from a dispatcher (Ay and Polani, 2008; Westrum, 2004), and is reliant on access to organizational assets and resources (Klein and Rai, 2009). Some researchers have attempted to understand the relationship between the sharing of information and decision-making and sharing the respective level of safety maintained by an organization (Gordon et al., 2003). According to Fair Information Practices, information secrecy factors include collection barriers, objective specifications, quality of data, usage limits, security, accountability, openness, and personal-level involvement (Westin, 1966; Zuo and Keefe, 2007).

The information flow within the organization can be considered a significant driver to reduce the firm’s informational breaches and to create safety (Westrum, 2014). It reflects the quality of decision-making, trust, and cooperation within the organization and its people. Hence, it allows the firm to access the components of cyber threats and also improves employees’ knowledge and awareness of new threats and facilitates them to recognize such threats (Fields et al., 2016; Li et al., 2019).

2.3 Training

Knowledge and training sessions have a dynamic impact on cyberspace and information security management within the organization, and also deliver awareness when employees have gained knowledge and skills for their jobs and performance (Wiley, McCormac, and

Calic, 2020). Security training and consciousness are recognized as some of the factual reasons for numerous failures in information and cyberspace security understanding and preparations. Until now, only a few studies have investigated the nature of security knowledge and awareness (Johnson, 2006; Li et al., 2019). Cyber and information security researchers have identified insiders as a major threat to the functioning of an effective cybersecurity program. In order to deal with insider risks, a firm needs to implement training and educational programs; security training should be given to advance knowledge and awareness (Straub and Welke, 1998; Zwilling et al., 2020), which helps transform people's attitudes and concerns regarding security (Johnson, 2006).

The need for management to have broad knowledge of information security and networks for employees within organizations has been acknowledged by many researchers (Abawajy, 2014; Cone et al., 2007; Fielt et al., 2013; Trkman and Desouza, 2012). Hence, employees generally undergo certification programs and training sessions. Training enhances knowledge and awareness in cybersecurity for the detection of cyber threats (Ben-Asher and Gonzalez, 2015; Berry and Berry, 2018). Organizations are required to share knowledge with each other if they want to improve cybersecurity and information management in the digital system.

2.4 Alliance and Collaboration

Over the past few years, it has been proved that collaborative security is an effective approach to identify cyber vulnerabilities and guard information (Singhal et al., 2013). More recently, research associated with security and collaboration has been drawing more attention (Jarvenpaa and Majchrzak, 2008; Smith et al., 2007). The increase in research on collaborative security management can be seen in the continuous increase in the number of research studies available in the recent years. Collaboration solutions are effective and successful in many domains of security and safeguarding, e.g., intrusion detection, anti-malware, recognition of cyberspace attackers, and threat detection; cybersecurity analysts are often reluctant to adopt collaborative solutions. Collaborative security can be defined as a joint venture between multiple safeguarding systems through the sharing of knowledge associated with security in order to make more effective and rational security and safeguarding decisions (Gaonkar and Viswanadham, 2001; Talja, 2002). Collaboration plays a prime role in the detection of spam and filtering (Hwang et al., 2011). Organizations should focus on collaboration as an opportunity to enhance cybersecurity and technology preparedness (Amrollahi and Rowlands, 2017). The aim of collaborative security and safeguarding is to share reliable information in order to offer enhanced security for large systems as compared to traditional, individual security; and it is more impactful and accurate in detecting threats and sophisticated attacks (Ključnikov, Mura, and Sklenár, 2019; Majchrzak, 2004; Meng et al., 2015).

2.5 Governance

Governance in the decision-making process within an organization, making the right decisions, and an accountability structure work to support desirable behavior in the management and operation of security (Gurbaxani and Whang, 1991; Ključnikov, Mura, and Sklenár, 2019). Effective governance in information and cybersecurity means that managers are able to allocate responsibilities (Dhillon and Torkzadeh, 2006; Papazafeiropoulou and Spanaki, 2016). The top management of organizations is responsible for considering and addressing the threat of cyber-attack; awareness (Zwilling et al., 2020) and action at the top level are vital to shape and support the governance structure of an organization (Li et al., 2019; Wedutenko et al., 2015). Improving cybersecurity prospects involves greater accountability in ascertaining how to control the growing level of power being exercised through cyberspace (Knox, 2018). The strategic approach to IT management should be backed by good corporate governance across any organization (Ključnikov, Mura, and Sklenár, 2019; Shollo et al., 2015).

2.6 Security Awareness

Security awareness is the main pillar of cyberspace for any organization (Zwilling et al., 2020) seeking to prevent major security breaches as complicated technologies are unlikely to avert cyber threats if workers and employees are not "conscious and aware" of the issues regarding cybersecurity (Dahbur et al., 2017; Wiley, McCormac, and Calic, 2020). Security awareness involves raising the development and maturity level of workers and developing their security responsibilities (Li et al., 2019; Stewart et al., 2015). Employees who follow the organization's safety rules and regulations can strengthen information security. Employees can become the strongest protection against security threats, with the right security awareness (Parsons et al., 2014). Training and security awareness programs can be more effective in implementing organizational cybersecurity systems (Valentine, 2006; Wiley, McCormac, and Calic, 2020).

2.7 Technological Infrastructure

Technological infrastructure is defined as the existing infrastructure and technologies working within a firm that is experiencing destructiveness, necessitating preservation and alleviation (Knapp et al., 2009). Cybersecurity depends on elements related to a firm's existing technological infrastructure and the compatibility of existing cyberspace security technologies with recent technologies and connected networks (Rowe et al., 2011). New vulnerabilities in current and existing technologies are exposed every day; even a well-considered policy cannot anticipate every newly generated risk and threat. Organizations and firms devise strategies with a preventive mindset to ascertain the availability of technology design and infrastructure and services rather than to protect the privacy of information and knowledge assets (Ahmad et al., 2014). Technological infrastructure addresses business processes and activities, data sets and information flows, software, and technology (Mendelson, 2000; Rowe et al., 2011).

Cybersecurity has become important for both public and non-public organizations due to significant dependency on information and communication technology (ICT). A better understanding of technological infrastructure, good governance, collaboration with technologically advanced organizations, and knowledge and awareness of cybersecurity are important factors for successful cybersecurity management within organizations. Many studies show that there is a significant impact of technological infrastructure on cybersecurity management (Byres and Hoffman, 2004; Klaic and Ph, 2015; Kwon and Johnson, 2012). Continuous maintenance of existing technological infrastructure helps to avoid future cyber threats within organizations. An organization can fulfil corporate cybersecurity requirements by implementing emerging technologies and other technological tools. The top management team can play an essential role in implementing cybersecurity management by offering necessary resources and support. Top management teams should be active in cybersecurity-management-related monitoring and decisions. They can provide training programs (Berry and Berry, 2018) on data/information protection and cybersecurity awareness programs (Li et al., 2019). Training programs can help in the exchange of knowledge and the flow of information within organizations (Wiley, McCormac, and Calic, 2020). Moreover, some researchers have explored the significant impact of good governance and top management support in the management of strategic collaborations with other technologically advanced companies to improve organizational resources and technical capabilities (Berry and Berry, 2018; Safa et al., 2018; Wiley, McCormac, and Calic, 2020). Collaboration can help to exchange knowledge, resources, skills, and expertise in order to resolve the increasing cybersecurity challenges within organizations (Ključnikov, Mura, and Sklenár, 2019).

Although several works have explored the significance of these identified factors in cybersecurity management, there is no detailed analysis of the interrelationships among these factors in the context of cybersecurity management. In this study, we will attempt to explore how these identified factors are related to each other and contribute to cybersecurity management within organizations. In view of the significance of this need, the study aims to explore the interrelationships among identified factors in cybersecurity management and to develop a hierarchical model. To meet the objectives of the study, we have used a modified total interpretive structural modeling (M-TISM) methodology and path analysis of the M-TISM model through different case studies.

3. Research Methodology

We used the M-TISM technique to achieve the research objectives of this study. The M-TISM is an advanced qualitative modeling technique, which has been widely used by researchers and practitioners in different areas of research (Dhir et al., 2020; Haleem et al., 2012; Srivastava and Sushil, 2013; Wasuja et al., 2012). It is a novel extension of interpretive structural modeling (ISM) (Warfield, 1974), which is used to develop a hierarchical structure of the factors in interest areas (Sushil, 2012; Sushil, 2017a; Sushil, 2018b). This methodology helps to deal with questions such as "what," "why," and "how" during the development of the hierarchical structure of the identified factors. While comparing M-TISM to the other different qualitative methodologies, bibliometric analysis and systematic literature review can help in identification of factors and various themes, but it will not help to develop a theoretical model of those factors. In addition to this, the decision-making trial and evaluation laboratory (DEMATEL) (Chang et al., 2011) can help to analyze the cause-and-effect interactions of the factors, but it also fails to develop the hierarchical structure of the factors. Again, comparing M-TISM with structural equation modeling (SEM) (Jena et al., 2017), SEM can be seen to help in statistical validation of a previously developed conceptual model, whereas M-TISM is an analytical method (Rajan, Dhir, and Sushil, 2020; Sushil, 2017b) that helps in the development of a new conceptual model in various contexts with the use of literature review and expert opinion. The M-TISM methodology (Rajan, Dhir, and Sushil, 2020) helps to identify critical factors, develop the contextual relationships among the identified factors, and construct a hierarchical model of the identified factors in an organized manner. This method also helps to explain the nature and interrelationships of the identified factors. In the M-TISM, the steps of TISM (Sushil, 2012) are combined into one step, where the researchers examine successive pairwise comparisons and check of transitivity (see Fig. 2). The pair of factors with transitional links need not be compared later in M-TISM. Therefore, M-TISM is used to reduce expert-based paired comparisons, and it helps to obtain a transitive reachability matrix in a single step (Sushil, 2017b; Sushil, 2018a). In this study, a total of seven factors have been identified using a literature review (see Table 1).

<<Insert Table 1 here>>

The various steps involved in the M-TISM process are explained below in a flowchart (see Fig. 1).

<<Insert Figure 1 here>>

Step 1: Identification of factors: This step involves the identification of the factors that affect cybersecurity management within the organization with the help of a comprehensive literature review. This process also involves an understanding of existing theories and literature in the given area of interest during the identification of critical factors.

Step 2: Definition of the contextual relationship between identified factors: The second step involves the description of the contextual relationships between the identified factors: “factor A will enhance or influence factor B,” and the same process needs to be carried out for all the factors and this is used to build the structure of the model. Example: “governance will affect collaboration” in the context of cybersecurity management within organizations.

Step 3: Interpretation of relationships among identified factors: This step involves interpretations of the relationship between each pair of factors with the help of a literature review. This step helps in achieving comprehensive knowledge of the subject domain. This step upgrades the ISM technique to M-ISM by providing an interpretation of the relationships among identified factors.

Step 4: Pairwise comparison of the identified factors: Pairwise comparison is used to develop an “interpretive logic-knowledge base.” In this step, all identified factors are compared, and each comparison is denoted by Y (Yes) or N (No). If the relationship between identified factors exists, it will be denoted by Y; and if the relationship between two factors does not exist, it will be denoted by N.

Step 5: Reachability matrix and checking the transitivity of factors: In this step, the reachability matrix is developed using an “interpretive logic-knowledge base.” Y and N codes from the “interpretive logic-knowledge base” are converted to 0 and 1, respectively. Lastly, the reachability matrix is checked for the transitivity rule. The rule of transitivity is as follows: “if A relates to B, and B relates to C, then A will be transitively related to C.” The transitivity check continues until the transitivity is fully examined. If we get a transitive connection, the “N” in the knowledge base will be replaced by “Y,” and the term “transitive” has to remain the same in the interpretation column.

Step 6: Hierarchical-level partition of factors: In this step, level partition is performed in the same way as the traditional TISM. This process is performed until the level of each factor is achieved. The determined level of each factor is used to develop the hierarchical structure.

Step 7: Drawing ISM digraph: The ISM digraph is developed based on the reachability matrix. This digraph consists of direct links and transitive links. These links show the established relationships between the identified factors in the respective domains. The arrows are employed in the links to show the direction of the relationships between the factors.

Step 8: Interaction (binary) matrix: The binary interaction matrix is developed using an ISM digraph with 1 and 0, where 1 shows the relationships between factors (direct and significant transitive links) and 0 indicates the absence of relationships.

Step 9: M-TISM model: The M-TISM model is developed from the matrix of interaction and the digraph. This also includes the interpretation of each link in the developed model.

3.1 M-TISM in the Context of Cybersecurity Management

The M-TISM technique has been used to build a hierarchical structure and examine relationships among seven factors in the context of cybersecurity management within the organization. Table 2 shows the seven identified factors, contextual relationships, and explanations for the elements of enablers of cybersecurity and management in organizations.

<<Insert Table 2 here>>

Fig. 2 shows the successive comparison digraph of the identified factors. The comparison between identified factors has been done in a sequential manner because initially the hierarchy of factors is not known. The successive comparison is based on the literature review.

<<Insert Figure 2 here>>

The reachability and transitive matrix has been developed using Fig. 2 (see Table 3).

<<Insert Table 3 here>>

The reachability sets and antecedent sets are developed (see Table 4) from the final reachability matrix (see Table 3). The reachability set contains the row elements, whereas the antecedent set shows the column elements of the final reachability matrix. The intersection set contains the common elements of the reachability set and antecedent set (Srivastava and Sushil, 2013). The factors that have similar reachability and intersection sets are put in the topmost-level group (Level I group) (see Table 4). Again, these top-level factors are eliminated in the next row of iteration, and the process is repeated until all levels of each factor are determined.

<<Insert Table 4 here>>

Table 4 shows the partitions of the reachability matrix (Table 3) based on the reachability set, antecedent set, and intersection set to place the identified factors level-wise. The reachability set consists of the row factors of the reachability matrix. The antecedent set consists of the column factors, while the intersection set consists of the common factors in the reachability set and antecedent set. If the intersection set is the same as the reachability set in the first iteration, then we place the factor at the top level. In the second iteration, we remove top-level factors from the set and continue the same procedure until the levels of all factors are obtained. Table 5 shows the different levels of identified factors that will help to build the hierarchical model.

<<Insert Table 5 here>>

The directed ISM digraph that has been developed shows the relationship between the factors according to their level. The direct line shows the direct relationships, and the dotted line shows the transitive relationships. The transitive links that have no relationship in the existing literature have been eliminated from the directed digraph (see Fig. 3).

<<Insert Figure 3 here>>

The information which was gathered from the reachability matrix (see Table 3) and digraph (see Fig. 3) is used to develop the binary matrix (see Table 6). The binary matrix contains 1 and 0 to show the links between the factors, where 1 indicates direct/transitive relations and 0 indicates the absence of a relationship between factors.

<<Insert Table 6 here>>

The interpretation of relationships among identified factors is very important to develop the M-TISM model. This step differentiates M-TISM from traditional ISM by interpreting the cause of the relationship among the identified factors and extracting in-depth knowledge about the area of research concerned. This step promotes understanding of “how factor A impacts factor B.” In this step, each factor is compared with other identified factors. In this study, the interaction matrix (see Table 7) has been developed based on supporting literature and the binary matrix (see Table 6). Finally, the hierarchical structure (M-TISM model) (see Fig. 4) of identified factors has been developed based on the ISM digraph (see Fig. 3) and the interpretive matrix (see Table 7).

<<Insert Table 7 here>>

<<Insert Figure 4 here>>

4. Validation of Paths of M-TISM using Cases

This study has determined the influential factors in organizational cybersecurity and shows that governance is a very significant variable for any organization. Top managers create strategic plans and cooperate with other organizations to reduce cyber threats (Ahmad et al., 2014). Therefore, governance and collaborations are correlated with each other. The same relationship is supported by the examples given below.

Path 1: Collaboration and Governance

Inter-firm alliances can be a process by which companies look at different aspects of a problem and find a possible solution (Kumar and Andersen, 2000; Safa et al., 2018). Leadership and the style of governance play a significant role in determining the solution to the problem through a strategic approach. Many strategic approaches are required by the top management team to manage the task structure and issues in organizations.

<<Insert Figure 5 here>>

Bharti Airtel is the largest telecom service provider in India, and Symantec Corp is a major global cybersecurity company. In 2017, both companies established a collaboration to meet the requirements of the growing cybersecurity business in India for cybersecurity and prevention of online threats (“Airtel and Symantec,” 2017). The objective of the alliance was to use security techniques to solve the challenges of cyber defense and to provide strong security to customers (Safa et al., 2018). Gopal Vittal, MD, and CEO (Bharti Airtel), said "We are delighted to collaborate with Symantec to guard against sophisticated cyber threats." Hence, the leadership must believe in the principles of alliancing culture and collaboration. Fig. 5 validates and justifies the finding of the M-TISM model in the current context of the study.

Path 2: Collaboration, Resources, Capabilities, and Technological Infrastructure

The collaboration supports the utilization of resources and capabilities and facilitates the flow of knowledge within the organization to achieve higher cybersecurity performance (Ključnikov, Mura, and Sklenár, 2019). The combination of firm-specific resources enhances the technological arrangements of the partner firms and helps the organization handle cyber threats appropriately.

<<Insert Figure 6 here>>

Bharti Airtel, India's largest telecom company, has collaborated with Seamless Alliance to provide uninterrupted high-speed and secure in-flight data connectivity to its customers. To offer safe data connectivity, the two companies have shared their resources to take advantage of satellite technology and to eliminate technical issues. Owing to the collaboration, more than 370 million mobile subscribers in Airtel's global network are able to use high-speed data services with optimal Internet experience ("Bharti Airtel Joins Global Collaboration," 2018). Thus, Fig. 6 validates and justifies the finding of a relationship between collaboration, resources, and capabilities, and technological infrastructure in the M-TISM model.

Path 3: Collaboration, Training, and Information Flow

Collaborations and alliances help increase employees' knowledge and experience through training programs (Ključnikov, Mura, and Sklenár, 2019). The aim was to educate the workforce and ensure the flow of information within the organization through training and knowledge-sharing programs (Atalay and Sarvan, 2014).

<<Insert Figure 7 here>>

An airport terminal and the aviation industry in Turkey have collaborated to explore knowledge management processes within organizations. The collaboration has provided knowledge to partner firms in the context of marketing, operations, environmental management systems, and security systems. Apart from this, partners with additional experience have transferred more knowledge, information, and technology to the airport management teams. Therefore, the airport has developed the performance of employees and gained a more competitive position in the market. The partner firms gain knowledge and know-how from each other through the agency of the international joint venture (Lane, Salk, and Lyles, 2001). Post-alliance partner firms have developed good communication networks among workers through knowledge (Safa et al., 2018) and skill development programs (Dhir et al., 2019; Wiley, McCormac, and Calic, 2020). The knowledge transfers and sharing undertaken in the collaboration were done through joint training and skill development programs for workers at the firms. Every year, airport management training is organized for managers by partner firms. The strategic collaboration has facilitated learning, knowledge, and the flow of information among the workers of partner firms in order to gain success in the competitive market. Therefore, Fig. 7 validates the finding of a relationship between collaboration, knowledge, and training, and information flow in the M-TISM model.

Path 4: Collaboration, Training, and Security Awareness

Collaboration helps in acquiring knowledge and skills, thereby increasing awareness of the workforce's cyber insecurity.

<<Insert Figure 8 here>>

Cisco and the UK police collaborated to enhance understanding of cybercrime attacks and to raise awareness among UK police through a cybersecurity training and skill development program (“Cisco Offers,” 2018). The Cisco Networking Academy planned to provide customized training to officers across Wales, Scotland, England, and Northern Ireland. This program helped more than police officers in the UK. The UK police were able to gain knowledge and awareness to defend networks. Police officers were able to close the knowledge gap and acquire new skills in the context of cyber and network threats (Murphy, 2018). Thus, Fig. 8 validates the finding of a relationship between collaboration, knowledge, and training, and security awareness in the M-TISM model.

5. Discussion of Findings

Cybersecurity management is becoming an important topic of discussion for both managers and practitioners. The M-TISM technique is effectively applied to identify and examine the interrelationships among various identified factors and develop a hierarchical model. From the M-TISM model developed, it is observed that there are important relationships that exist between the identified factors in this study. The M-TISM model developed shows the hierarchical structure and relationships of the seven identified factors in the context of cybersecurity management within organizations. The direction of each relationship was established based on the literature review. Governance (C5), alliance and collaboration (C4), training (C3), resources and capabilities (C1), information flow (C2), security awareness (C6), and technological infrastructure (C7) are critical factors for cybersecurity management within organizations. Governance (C5) lies at the lowest level in the M-TISM model and can be considered the most important factor in cybersecurity management, followed by alliances and collaborations (C4). These factors have strong driving power in the developed model and play a significant role in cybersecurity management within organizations. Good governance by the senior management team is the most critical factor for influencing cybersecurity effectiveness and maximizing information security protection within organizations (Zafar, Ko, and Osei-Bryson, 2016). Top management teams can also help in creating and updating cybersecurity policies for an organization (Jenab and Moslehpour, 2016). The results show that governance enhances cybersecurity by providing financial support, effective cybersecurity policies, learning culture, and involvement in initiatives on information security within organizations (McCormac and Calic, 2020).

Top management should also support and promote strategic alliances and collaborations (Ključnikov, Mura, and Sklenár, 2019) with other technologically advanced organizations in order to promote skill development of employees and teamwork for achieving cybersecurity goals. Alliances and collaborations promote training programs, facilitate learning from allied organizations, and build a security-friendly culture within organizations (Safa et al., 2018). Collaborations can improve information-sharing and help to develop the existing infrastructure of software and applications (Happa, Glencross, and Steed, 2019; Ključnikov, Mura, and Sklenár, 2019). Alliances can help to enhance the knowledge (Bindra, Parameswar, and Dhir, 2019; Bindra et al., 2020; Sharma et al., 2020a; 2020b) and experience of employees within organizations. They also bring in complementary resources and facilitate the flow of knowledge in order to secure organizational information. They also help in the development of the resources and capabilities of the organization (Safa et al., 2018). The development of organizational resources and capabilities can influence the effectiveness of organizational cybersecurity programs.

Collaboration and alliances also help to develop the technological infrastructure that is required for the regular updating and assessment of information security practices within organizations. Training also helps in the creation of cybersecurity awareness (Li et al., 2019) among employees and increases the level of consciousness about sharing sensitive information (Berry and Berry, 2018). Training programs on cybersecurity can help to develop the knowledge and skills of employees in order to increase their security awareness (Wiley, McCormac, and Calic, 2020). This helps to manage the confidentiality of information and identify new vulnerabilities and external threats in order to respond quickly. This study makes a theoretical as well as a managerial contribution. From the theoretical viewpoint, this study has developed a hierarchical structure of all identified factors in cybersecurity management. From the practical viewpoint, this study sends a strong message to cybersecurity practitioners about the need to have good governance to ensure effective cybersecurity management within organizations.

5.1 Theoretical Contributions

In this study, the M-TISM model was developed in the context of cybersecurity management. M-TISM models have been used in various areas of research and address the questions of theory-building, such as “what,” “why,” and “how” (Sushil, 2017). The findings of the study show that resources and capabilities have an important role in cybersecurity management. Hence, this contributes to the resource-based view (Barney, Wright, and Ketchen Jr, 2001). This theory states that an organization’s resources and technological capabilities have a positive impact on organizational security performance (Chae et al., 2014). A strategic alliance with other technological organizations can help in the development of resources and technological skills (Safa et al., 2018). Collaboration with other organizations can serve as a catalyst for the technological infrastructure development of the organization, which will directly help in cybersecurity management (Dhillon et al., 2017; Happa, Glencross, and Steed, 2019). This study also enriches organizational learning theory. The M-TISM model developed shows that an organization can improve its learning and expertise through collaboration and training. The M-TISM model can be used to understand and explore the various critical factors in cybersecurity management. The findings indicate that resources and capabilities, information flow, training, alliances and collaborations, governance, security awareness, and technological infrastructure play a crucial role in cybersecurity management. Further, empirical validation is required to determine whether the identified factors have a positive or negative impact on organizational cybersecurity performance.

5.2 Managerial Implications

This study offers several managerial contributions. It is very useful for practitioners, as it confirms that an organization can enhance its cybersecurity management by focusing on significant factors and the M-TISM model developed. The M-TISM model developed shows that organizational security can be enhanced by good governance within an organization. Top management can help in setting up basic rules and regulations under which a strategic alliance (Dhillon et al., 2017) and partnership between technological organizations can take place in order to improve cybersecurity management. Good governance facilitates mediation for the collaborative process (Ansell and Gash, 2008). Thus, managers can enhance their cybersecurity strategy by focusing on sharing knowledge and experience and providing good management support. Collaboration can help to enhance the knowledge and skill of employees, which can result in smooth information flow among employees and can enhance cybersecurity awareness (de Vreede et al., 2016; Li et al., 2019; Siponen, 2000). Collaboration can help to develop cybersecurity techniques, motivate employees, increase awareness, encourage risk-sharing, and facilitate a healthy organizational culture (Happa, Glencross, and Steed, 2019). These features are crucial for the creation of security awareness (Reay et al., 2013; Siponen, 2000). Resources related to IT, such as technological infrastructure and employee skills, are tightly connected to cybersecurity management. These dimensions can help managers to integrate cybersecurity planning within organizations. Good technological infrastructure can leverage the resources and capabilities of emerging information applications and technologies (Chuang and Lin, 2013). The manager can restructure existing cybersecurity strategies and introduce effective mechanisms, which include design and planning, new business applications delivery, and planning for cybersecurity standards and controls in order to ensure a secure flow of information and data within the organization. From a practical point of view, this study is very important for managers and practitioners to decide which factors they should consider in their cybersecurity strategy and make managerial decisions. The study also suggests that a manager can better evaluate the organization's preparedness for cybersecurity management by considering the M-TISM model. Thus, managers should be aware of the dynamic issues and factors in the security information within the organization. This study will facilitate managers to implement cybersecurity operations. The M-TISM model developed provides a clear picture regarding the impact of various factors on cybersecurity management and performance. The top management team should enhance organizational security awareness among employees. This will help to encourage constructive attitudes and behavior toward cybersecurity. Likewise, top managers should encourage their employees to share new knowledge and technical skills with partner firms.

6. Proposed Theoretical Model and Propositions

In this section, we discuss possible research opportunities in the area of cybersecurity management. Future researchers will be inspired to empirically test the proposed model (see Fig. 9) and develop theory in the field of cybersecurity management. Based on the literature review and findings, we have developed a total of nine propositions, which can be tested in future studies through the lens of cybersecurity management.

Top managers play a vital role in cybersecurity management (Iovan and Iovan, 2016). The senior-level management team is responsible for holistic strategies, prioritizing investments (Franke and Brynielsson, 2014), better utilization of organizational resources, and establishing the standards and governance framework that are required for cybersecurity management (Knowles et al., 2015). Hence, top management support can be a critical factor affecting cybersecurity management within organizations. Several studies have examined the significant impact of top management support on information security management (Hu et al., 2012;

Ključnikov, Mura, and Sklenár, 2019), information security knowledge management (Abdullah, Uli, and Mohamed, 2014), information system security effectiveness, employee security awareness (Tsohou et al., 2015), and training (Soomro, Shah, and Ahmed, 2016).

<<Insert Figure 9 here>>

Although researchers have examined the impact of top management support on the formation of technological alliances (Sampson, 2007) and collaborations (Lee and Park, 2008; Montoya-Torres and Ortiz-Vargas, 2014), very little is known about how top management support affects the outcomes of technical collaboration in the context of cybersecurity management within organizations. Based on the discussion, we suggest the following proposition:

Proposition 1. Top management support will have a positive impact on strategic alliance formation in the context of cybersecurity management.

Past studies have revealed the significance of strategic alliances and technology collaborations on skill development (Oviawe, Uwameiye, and Uddin, 2017; Summers and Barber, 2003) and improved information security performance (Stewart and Jürjens, 2017). Many studies have examined the impact of technological alliances and collaborations on knowledge and skill development (Haqaf and Koyuncu, 2018; Oviawe, Uwameiye, and Uddin, 2017; Summers and Barber, 2003); however, a very limited number of studies have examined the relationship between technological alliances and skill development through training (Buchler et al., 2018; Cains et al., 2021; Caldwell, 2013) in the context of cybersecurity management. Although a few studies have highlighted the significance of technological collaboration on knowledge development (Kritzinger and Von Solms, 2012; Kshetri, 2013), very little is known about how they help in skill development in the context of cybersecurity management within organizations. Based on the discussion, we suggest the following proposition:

Proposition 2. Alliances and collaborations will have a positive effect on training and skill development in the context of cybersecurity management.

According to the previous literature, there has been a significant increase in strategic alliances and collaborations (Buchler et al., 2018; Cains et al., 2021; Caldwell, 2013) to improve employee productivity and skills and reduce the risk of cyber threats within organizations. Most organizations use strategic alliances as a strategy for business expansion and organizational performance (Haqaf and Koyuncu, 2018; Oviawe, Uwameiye, and Uddin, 2017). These collaborations help allied organizations to develop their R&D capabilities, innovation capabilities (Dinesh and Sushil, 2021; Haqaf and Koyuncu, 2018), skill development (Summers and Barber, 2003), and sharing of technological resources, knowledge, and capabilities (Naicker and Mafaiti, 2019). Many studies have examined the role of strategic alliances in developing resources, technical capabilities, resource integration (Naicker and Mafaiti, 2019), and organizational performance (Buchler et al., 2018). The literature review indicates that many scholars have explored the significance of strategic alliances in developing alliance capabilities, inter-partner attributes, performance outcomes, firm innovation (Stuart, 2000), and resource management (Aral and Weill, 2007). A strategic alliance enables an organization to improve its performance (Stuart, 2000) by combining technological resources and skills with those of other technological firms. Technological resources and capabilities are critical factors for improvement in the firm's performance and they create valuable outcomes from partnerships (Kafouros et al., 2015). However, less research has been undertaken to explain the role of technological resources in organizational cybersecurity performance after the formation of a strategic alliance (He et al., 2020). Based on the above discussion, we suggest the following proposition:

Proposition 3: Alliances and collaborations will have a positive effect on development of resources and capabilities in the context of cybersecurity management.

Security awareness is considered a crucial factor for any organization dealing with cybersecurity management (Von Solms and Van Niekerk, 2013; Zwilling et al., 2020). Many scholars have examined the role of strategic alliances and collaborations in security awareness

(Safa, Von Solms, and Furnell, 2016) and information security behavior (Safa et al., 2017). Several studies have examined the human aspects of cyber and information security management within the organization (Safa et al., 2015; Safa et al., 2017). Organizations form a strategic alliance with other technologically advanced firms to gain information security knowledge and experience. Many scholars have suggested that strategic collaborations have a significant impact on security awareness (Cains et al., 2021; Safa et al., 2017; Von Solms and Van Niekerk, 2013) and on employees' attitudes regarding information and cybersecurity management. Employees can gain new information about misleading applications and software and many other information and cybersecurity breaches from partner firms (Crossler et al., 2013). Security awareness in such organizations can help to mitigate the effect of a cyber-attack (Sohrabi Safa et al., 2018). Many studies show the role of collaboration and partnership in information security management (Safa et al., 2017; Safa et al., 2018; Von Solms and Van Niekerk, 2013). Studies also show the role of employee attitude and security awareness in the mitigation of information security risk within organizations (Chen, Shaw, and Yang, 2006; Safa et al., 2016). Only a few studies have examined the role of security awareness in cybersecurity management within organizations (Abawajy, 2014; Zwilling et al., 2020). Based on the above discussion, we suggest the following proposition:

Proposition 4: Alliances and collaborations will have a positive effect on security awareness in the context of cybersecurity management.

Advancement in technological infrastructure has been seen as an important factor for improved organizational cybersecurity performance (Ani, He, and Tiwari, 2017). Various studies have examined the role of strategic alliances in the development of technological infrastructure and capabilities (Haeussler, Patzelt, and Zahra, 2012; Venkatraman, Henderson, and Oldach, 1993). Many organizations struggle to perform better in the competitive market due to lack of technological infrastructure, including technological resources, capabilities, skills, and knowledge (Haeussler, Patzelt, and Zahra, 2012). Many researchers suggest that external technological capabilities and resources gained from partnership with technologically advanced organizations are helpful in the development of the technological infrastructure and industry-relevant capabilities, skills, and knowledge (Haeussler, Patzelt, and Zahra, 2012; Martínez-Noya and García-Canal, 2011) of an allied firm. Technological infrastructure developed from strategic alliances impacts technological innovation (Dinesh and Sushil, 2019), and organizational performance (Srivastava, Gnyawali, and Hatfield, 2015). Few studies have examined the role of technological infrastructure in information security management (Soomro, Shah, and Ahmed, 2016; Von Solms and Van Niekerk, 2013). Despite various studies in the area of cybersecurity management, little attention has been given to the role of technological infrastructure in cybersecurity performance. Based on the discussion, we suggest the following proposition:

Proposition 5: Alliances and collaborations will have a positive effect on the development of the technological infrastructure of allied firms in the context of cybersecurity management.

Many scholars have investigated the significant impact of staff training in effective cybersecurity management through skill development and cybersecurity awareness (Chang and Yeh, 2006; Li et al., 2019) within organizations (Hart et al., 2020). The literature on cybersecurity management also contains discussion around cybersecurity policy development, training (Hart et al., 2020), and cybersecurity policy awareness (Zwilling et al., 2020). Many studies have shown that cybersecurity training helps to increase awareness (Zwilling et al., 2020), cybersecurity culture (Alshaikh, 2020), and employees' understanding of cybersecurity management (Abawajy, 2014; Kahyaoglu and Caliyurt, 2018). Previously, cybersecurity management issues were studied in the context of cybersecurity policies (De Bruijn and Janssen, 2017), employees' cybersecurity behavior (Zwilling et al., 2020), employee engagement (Alshaikh, 2020), organizational cybersecurity culture (Abawajy, 2014), and skill development (Kahyaoglu and Caliyurt, 2018). Several studies have explored the significant role of training in the information security management context (Kazemi, Khajouei, and Nasrabadi, 2012; Singh, Gupta, and Ojha, 2014; Soomro, Shah, and Ahmed, 2016), but little research has been undertaken to explore the role of strategic alliances and collaborations in training to enhance organizational cybersecurity performance (Hart et al., 2020). Based on the discussion, we suggest the following proposition:

Proposition 6: Training will have a positive effect on organizational cybersecurity performance through skill development and knowledge.

Resources and capabilities have been recognized as valuable assets to ensure effective cybersecurity management within organizations (Chen, Chong, and Zhang, 2004; Ferdinand, 2015). Resources include knowledge, technological assets, organizational resources, and human and physical resources (Diaz-Diaz, Aguiar-Diaz, and De Saa-Perez, 2006; Freeze and Kulkarni, 2007), whereas capabilities include expertise and technical skills of employees within organizations (Fink and Neumann, 2007; Parmigiani and Mitchell, 2009). Previously, cybersecurity management issues were studied in the context of communication, awareness (Von Solms and Van Niekerk, 2013; Zwilling et al., 2020), cybersecurity culture (Alshaikh, 2020), human capital management, and knowledge management (Wang and Wang, 2019). Several studies have shown the significant impact of resources and capabilities in information security management (Chang, Chen, and Chen, 2011; Hall, Sarkani, and Mazzuchi, 2011; Kim, Kim and Seo, 2020), but relatively few of them have explored the role of resources and capabilities in the context of organizational cybersecurity performance (Naseer, Maynard, and Desouza, 2021). Hence, there is a need for empirical work to explore the impact of resources and capabilities on organizational cybersecurity performance. Based on the discussion, we suggest the following proposition:

Proposition 7: Resources and capabilities will have a positive effect on organizational cybersecurity performance.

Several studies have examined the role of top management support (Ključnikov, Mura, and Sklenár, 2019), security policy, technological architecture (Dawson, 2018), training, employee attitude, IT infrastructure, skill development (Wiley, McCormac, and Calic, 2020), and security awareness (Li et al., 2019) in information security management. Only a few studies have examined the role of security awareness in cybersecurity management within organizations (Abawajy, 2014; Zwilling et al., 2020). Security awareness plays a vital role in developing an organization's technological architecture and resolving security issues related to cybersecurity within organizations (Chang and Yeh, 2006; Li et al., 2019). Many scholars have examined that separately from technological infrastructure, top management support (Ključnikov, Mura, and Sklenár, 2019), resources, technological capabilities (Chae et al., 2014), collaborations (Berry and Berry, 2018; Safa et al., 2018), and cybersecurity awareness (Li et al., 2019) among employees, which are also very significant factors for effective cybersecurity performance within organizations. Based on the discussion, we suggest the following proposition:

Proposition 8: Security awareness will have a positive effect on organizational cybersecurity performance.

Technological infrastructure has been considered the most significant factor in information management as well as cybersecurity management within organizations (Dawson, 2018; Von Solms and Van Niekerk, 2013). Both the private sector and the public sector use advanced technologies such as hardware devices and the latest security software to improve cybersecurity within organizations (Ahmad at al., 2020; Srinivas, Das, and Kumar, 2019). Although several studies have examined the role of IT infrastructure and technological architecture in information security management (Chang, Chen, and Chen, 2011; Hall, Sarkani, and Mazzuchi, 2011; Soomro, Shah, and Ahmed, 2016), only a few studies have examined the impact of technological infrastructure on cybersecurity management and performance (Boiko, Shendryk, and Boiko, 2019). Based on the discussion, we suggest the following proposition:

Proposition 9: Technological infrastructure will have a positive effect on organizational cybersecurity performance by improving technological resources and assets.

7. Limitations and Future Research Scope

This study suggests opportunities to carry out further research in organizational information and cybersecurity in the strategic information management field. In this study, empirical data is missing. The identified factors can further be validated through empirical analysis. The weakness of this study provides future research directions. Future research can investigate the wider aspects of organizational cybersecurity. We can perform a systematic literature review and identification of factors by using meta-analysis. Many other different factors can be identified in the context of cybersecurity and information management to develop a conceptual framework. Future research can examine the interrelationships between the identified factors, but greater empirical evidence will be required. We also encourage future researchers to use a more mixed approach to conducting cybersecurity research in order to validate their results and findings.

8. Conclusion

In this study, we have identified and examined the critical factors that lead to effective cybersecurity management within the organization. A hierarchical model of identified factors was developed using the M-TISM methodology. This model shows the hierarchy of and interrelationships between the identified factors in the context of cybersecurity within organizations. The various paths in the developed model have been validated in various cases. The findings suggest that governance has the most crucial impact on cybersecurity management, followed by alliances and collaborations. These factors have a strong driving power and play a crucial role in cybersecurity management within organizations. The other critical factors, i.e., training, resources and capabilities, information flow, security awareness, and technological infrastructure (Dawson, 2018), also play an important role in cybersecurity management within organizations. Top management can support strategic alliances and collaborations (Happa, Glencross, and Steed, 2019) with other technologically advanced organizations in order to gain skills and external knowledge to learn about best practices for cybersecurity management (Dhillon et al., 2017). Training and knowledge-sharing sessions can be organized across teams and organizations for dealing with cybersecurity threats. Effective training can lead to information flow and security awareness (Li et al., 2019) to address the growing cybersecurity threats within organizations. This study contributes to the theory of information security by showing how knowledge and information can be developed and utilized for cybersecurity management through training and collaboration.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 237-248.

Abdullah, H., Uli, J., & Mohamed, Z. A. (2014). Relationship between organizational characteristics and information security knowledge management implementation. Procedia-Social and Behavioral Sciences, 123, 433-443.

Abomhara, M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1), 65-88.

Ackoff, R. L. (1989). From data to wisdom. Journal of Applied Systems Analysis, 16(1), 3-9.

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. Journal of the Association for Information Science and Technology, 71(8), 939-953.

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: towards an organizational multi-strategy perspective. Journal of Intelligent Manufacturing, 25(2), 357-370.

Airtel and Symantec announce strategic partnership to offer leading cyber security solutions to businesses in India (2017). Retrieved from https://www.airtel.in/press-release/08-2017/airtel-and-symantec-announce-strategic-partnership-to-offer-leading-cyber-security-solutions-to-businesses-in-india/ Accessed on July 2020.

Akella, R., Tang, H., & McMillin, B. M. (2010). Analysis of information flow security in cyber–physical systems. International Journal of Critical Infrastructure Protection, 3(3-4), 157-173.

Ali, S. M., Arafin, A., Moktadir, M. A., Rahman, T., & Zahan, N. (2018). Barriers to reverse logistics in the computer supply chain using interpretive structural model. Global Journal of Flexible Systems Management, 19(1), 53-68.

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003.

Amit, R., & Schoemaker, P. J. (1993). Strategic assets and organizational rent. Strategic Management Journal, 14(1), 33-46.

Amrollahi, A., & Rowlands, B. (2017). Collaborative open strategic planning: a method and case study. Information Technology & People, 30(4), 832-852.

Ani, U. P. D., He, H., & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. Journal of Cyber Security Technology, 1(1), 32-74.

Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. Journal of Public Administration Research and Theory, 18(4), 543-571.

Aral, S., & Weill, P. (2007). IT assets, organizational capabilities, and firm performance: How resource allocations and organizational differences explain performance variation. Organization science, 18(5), 763-780.

Atalay, M., & Sarvan, F. (2014). Knowledge management processes in international joint ventures: A case of an airport operator firm. Procedia - Social and Behavioral Sciences, 150, 658-667.

Ay, N., & Polani, D. (2008). Information flows in causal networks. Advances in Complex Systems, 11(01), 17-41.

Barney, J., Wright, M., & Ketchen Jr, D. J. (2001). The resource-based view of the firm: Ten years after 1991. Journal of management, 27(6), 625-641.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. Computers in Human Behavior, 48, 51-61.

Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for cyber security threats. International Journal of Business Continuity and Risk Management, 8(1), 1-10.

Bharti Airtel joins global collaboration to bring high-speed in-flight data connectivity to mobile users (2018). Retrieved from https://www.businesstoday.in/technology/news/bharti-airtel-joins-global-collaboration-bring-high-speed-in-flight-data-connectivity-mobile-users/story/271479.html. Accessed on March 2020.

Bhawan, V., & Marg, S. J. S. (2005). Interpretive matrix: a tool to aid interpretation of management and social research. Global Journal of Flexible Systems Management, 6(2), 27-30.

Bieda, D., & Halawi, L., (2015). Cyberspace: A venue for terrorism. Issues in Information Systems, 16(3), 33.

Bindra, S., Parameswar, N. and Dhir, S. (2019), "Strategic management: The evolution of the field", Strategic Change, Vol. 28 No. 6, pp. 469-478.

Bindra, S., Srivastava, S., Sharma, D. and Ongsakul, V. (2020), "Reviewing knowledge-based dynamic capabilities: perspectives through meta-analysis", Journal for Global Business Advancement, Vol. 13 No. 3, pp. 273-295.

Blake, E. A. (2007). Network and database security: Regulatory compliance, network, and database security-a unified process and goal. Journal of digital forensics, security and law, 2(4), 5.

Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: uncertainties, risks and cyber security. Procedia computer science, 149, 65-70.

Buchler, N., La Fleur, C. G., Hoffman, B., Rajivan, P., Marusich, L., & Lightner, L. (2018). Cyber teaming and role specialization in a cyber security defense competition. Frontiers in psychology, 9, 2133.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523-548.

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2021). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. Risk Analysis.

Caldwell, T. (2013). Plugging the cyber-security skills gap. Computer Fraud & Security, 2013(7), 5-10.

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

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, 9(1), 70-104.

Chae, B. K., Yang, C., Olson, D., & Sheu, C. (2014). The impact of advanced analytics and data accuracy on operational performance: A contingent resource based theory (RBT) perspective. Decision support systems, 59, 119-126.

Chander, M., Jain, S. K., & Shankar, R. (2013). Modeling of information security management parameters in Indian organizations using ISM and MICMAC approach. Journal of Modelling in Management.

Chang, A. J. T., & Yeh, Q. J. (2006). On security preparations against possible IS threats across industries. Information Management & Computer Security.

Chang, B., Chang, C. W., & Wu, C. H. (2011). Fuzzy DEMATEL method for developing supplier selection criteria. Expert systems with Applications, 38(3), 1850-1858.

Chang, S. E., Chen, S. Y., & Chen, C. Y. (2011). Exploring the relationships between IT capabilities and information security management. International Journal of Technology Management, 54(2-3), 147-166.

Chaudhry, P. E., Chaudhry, S., & Reese, R. (2012). Developing a Model for Enterprise Information Systems Security. Economics, Management & Financial Markets, 7(4), 587-599.

Chen, C. C., Shaw, R. S., & Yang, S. C. (2006). Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. Information Technology, Learning & Performance Journal, 24(1).

Chen, Y. S., Chong, P. P., & Zhang, B. (2004). Cyber security management and e-government. Electronic Government, an International Journal, 1(3), 316-327.

Chuang, S. H., & Lin, H. N. (2013). The roles of infrastructure capability and customer orientation in enhancing customer-information quality in CRM systems: Empirical evidence from Taiwan. International Journal of Information Management, 33(2), 271-281.

Cisco Offers cyber training to UK police officers (2018). Retrieved from https://www.infosecurity-magazine.com/news/cisco-offers-cyber-training-uk/ Accessed on February 2020.

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. Computers & Security, 26(1), 63-72.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. computers & security, 32, 90-101.

Cyber Security Breaches Survey 2018. Available at. https://www.gov.uk/government/news/new-figures-show-large-numbers-of-businesses-and-charities-suffer-at-least-one-cyber-attack-in-the-past-year. Accessed January 2021.

Cyber Security Report 2020, National Technology Security Coalition (NTSC). Available at. https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf. Accessed January 2021.

Dahbur, K., Bashabsheh, Z., & Bashabsheh, D. (2017). Assessment of security awareness: A qualitative and quantitative study. International Management Review, 13(1), 37-58.

David, D. P., Keupp, M. M., & Mermoud, A. (2020). Knowledge absorption for cyber-security: The role of human beliefs. Computers in Human Behavior, 106, 106255.

Dawes, S. S. (2008). The evolution and continuing challenges of e-governance. Public Administration Review, 68(1), 86-102.

Dawson, M. (2018). Applying a holistic cybersecurity framework for global IT organizations. Business Information Review, 35(2), 60-67.

De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. Government Information Quarterly, 34(1), 1-7.

de Vreede, G. J., Antunes, P., Vassileva, J., Gerosa, M. A., & Wu, K. (2016). Collaboration technology in teams and organizations: Introduction to the special issue. Information Systems Frontiers, 18(1), 1-6.

Dhillon, G., & Torkzadeh, G. (2006). Value‐focused assessment of information system security in organizations. Information Systems Journal, 16(3), 293-314.

Dhillon, G., Syed, R., & de Sá-Soares, F. (2017). Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors. Information & Management, 54(4), 452-464.

Dhir, S. (2017). Flexibility in modification and termination of cross-border joint ventures. Global Journal of Flexible Systems Management, 18(2), 139-151.

Dhir, S., Ongsakul, V., Ahmed, Z. U., & Rajan, R. (2019). Integration of knowledge and enhancing competitiveness: A case of acquisition of Zain by Bharti Airtel. Journal of Business Research.

Diaz-Diaz, N. L., Aguiar-Diaz, I., & De Saa-Perez, P. (2006). Technological knowledge assets and innovation. International Journal of Technology Management, 35(1-4), 29-51.

Dinesh, K. K., & Sushil. (2019). Strategic innovation factors in startups: results of a cross-case analysis of Indian startups. Journal for Global Business Advancement, 12(3), 449-470.

Dinesh, K. K., & Sushil. (2021). Strategic innovation and entrepreneurial ownership: an analysis using GEM data and fuzzy simulation. Benchmarking: An International Journal.

Ekelund, S., & Iskoujina, Z. (2019). Cybersecurity economics–balancing operational security spending. Information Technology & People.

Farn, K. J., Lin, S. K., & Fung, A. R. W. (2004). A study on information security management system evaluation—assets, threat and vulnerability. Computer Standards &

Interfaces, 26(6), 501-513.

Ferdinand, J. (2015). Building organisational cyber resilience: a strategic knowledge-based view of cyber security management. Journal of business continuity & emergency planning, 9(2), 185-195.

Fielt, E., Böhmann, T., Korthaus, A., Conger, S., & Gable, G. (2013). Service management and engineering in information systems research. The Journal of Strategic Information Systems, 22(1), 46-50.

Fink, L., & Neumann, S. (2007). Gaining agility through IT personnel capabilities: The mediating role of IT infrastructure capabilities. Journal of the Association for Information Systems, 8(8), 25.

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness–a systematic review of the literature. Computers & Security, 46, 18-31.

Freeze, R. D., & Kulkarni, U. (2007). Knowledge management capability: defining knowledge assets. Journal of Knowledge management.

Gaonkar, R., & Viswanadham, N. (2001). Collaboration and information sharing in global contract manufacturing networks. IEEE/ASME Transactions on Mechatronics, 6(4), 366-376.

Gilmour, S., (2014). Policing crime and terrorism in cyberspace: An overview. The European Review of Organised Crime, 1(1), 143-159.

Gonçalves, M. J. A., Rocha, Á., & Cota, M. P. (2016). Information management model for competencies and learning outcomes in an educational context. Information Systems Frontiers, 18(6), 1051-1061.

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. Journal of Accounting and Public Policy, 22(6), 461-485.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. Communications of the ACM, 46(3), 81-85

Grant, R. M. (1991). The resource-based theory of competitive advantage: implications for strategy formulation. California Management Review, 33(3), 114-135.

Gurbaxani, V., & Whang, S. (1991). The impact of information systems on organizations and markets. Communications of the ACM, 34(1), 59-73.

Haeussler, C., Patzelt, H., & Zahra, S. A. (2012). Strategic alliances and product development in high technology new firms: The moderating effect of technological capabilities. Journal of business venturing, 27(2), 217-233.

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. Information Management & Computer Security.

Haleem, A., Sushil, Qadri, M. A., & Kumar, S. (2012). Analysis of critical success factors of world-class manufacturing practices: an application of interpretative structural modelling and interpretative ranking process. Production Planning & Control, 23(10-11), 722-734.

Hall, J. H., Sarkani, S., & Mazzuchi, T. A. (2011). Impacts of organizational capabilities in information security. Information Management & Computer Security.

Happa, J., Glencross, M., & Steed, A. (2019). Cyber security threats and challenges in collaborative mixed-reality. Frontiers in ICT, 6, 5.

Haqaf, H., & Koyuncu, M. (2018). Understanding key skills for information security managers.

International Journal of Information Management, 43, 165-172.

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. Computers & Security, 95, 101827.

He, Q., Meadows, M., Angwin, D., Gomes, E., & Child, J. (2020). Strategic alliance research in the era of digital transformation: Perspectives on future research. British Journal of Management, 31(3), 589-617.

Hota, C., Upadhyaya, S., & Al-Karaki, J. N. (2015). Advances in secure knowledge management in the big data era. Information Systems Frontiers, 17(5), 983-986.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4), 615-660.

Hwang, G. J., Shi, Y. R., & Chu, H. C. (2011). A concept map approach to developing collaborative Mindtools for context-aware ubiquitous learning. British Journal of Educational Technology, 42(5), 778-789.

Iovan, S., & Iovan, A. A. (2016). From cyber threats to cyber-crime. Journal of Information Systems & Operations Management, 425.

Jarvenpaa, S. L., & Majchrzak, A. (2008). Knowledge collaboration among professionals protecting national security: Role of transactive memories in ego-centered knowledge networks. Organization Science, 19(2), 260-276.

Jena, J., Sidharth, S., Thakur, L. S., Pathak, D. K., & Pandey, V. C. (2017). Total interpretive structural modeling (TISM): approach and application. Journal of Advances in Management Research.

Jenab, K., & Moslehpour, S. (2016). Cyber security management: A review. Business Management Dynamics, 5(11), 16.

Johnson, E. C. (2006). Security awareness: switch to a better programme. Network Security, 2006(2), 15-18.

Kafouros, M., Wang, C., Piperopoulos, P., & Zhang, M. (2015). Academic collaborations and firm innovation performance in China: The role of region-specific institutions. Research Policy, 44(3), 803-817.

Kahyaoglu, S. B., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. Managerial Auditing Journal.

Kazemi, M., Khajouei, H., & Nasrabadi, H. (2012). Evaluation of information security management system success factors: Case study of Municipal organization. African Journal of Business Management, 6(14), 4982-4989.

Kim, S., Kim, B., & Seo, M. (2020). Impacts of Sustainable Information Technology Capabilities on Information Security Assimilation: The Moderating Effects of Policy—Technology Balance. Sustainability, 12(15), 6139.

Klein, R., & Rai, A. (2009). Interfirm strategic information flows in logistics supply chain relationships. MIS Quarterly, 735-762.

Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: factors of success. Entrepreneurship and Sustainability Issues, 6(4), 2081.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: management's effect on culture and policy. Information Management & Computer Security.

Knapp, K. J., Morris Jr, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. Computers & Security, 28(7), 493-508.

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. International journal of critical infrastructure protection, 9, 52-80.

Knox, B. J. (2018). The Effect of Cyberpower on Institutional Development in Norway. Frontiers in Psychology, 1-9.

Kortjan, N., & Von Solms, R. (2014). A conceptual framework for cyber-security awareness and education in SA. South African Computer Journal, 52(1), 29-41.

Kritzinger, E., & Von Solms, S. H. (2012). A framework for cyber security in Africa. Journal of Information Assurance & Cybersecurity, 2012, 1.

Kshetri, N. (2013). Cybercrime and cyber-security issues associated with China: some economic and institutional considerations. Electronic Commerce Research, 13(1), 41-69.

Kumar, R., & Andersen, P. H. (2000). Inter firm diversity and the management of meaning in international strategic alliances. International Business Review, 9(2), 237-252.

Lane, P. J., Salk, J. E., & Lyles, M. A. (2001). Absorptive capacity, learning, and performance in international joint ventures. Strategic Management Journal, 22(12), 1139-1161.

Lee, H. U., & Park, J. H. (2008). The influence of top management team international exposure on international alliance formation. Journal of Management Studies, 45(5), 961-981.

Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet, 12(9), 1-21.

Leidner, D. E. (2010). Globalization, culture, and information: Towards global knowledge transparency. The Journal of Strategic Information Systems, 19(2), 69-77.

Leidner, D. E., & Kayworth, T. (2006). A review of culture in information systems research: Toward a theory of information technology culture conflict. MIS Quarterly, 30(2), 357-399.

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, 13-24.

Liao, R., Balasinorwala, S., & Rao, H. R. (2017). Computer assisted frauds: An examination of offender and offense characteristics in relation to arrests. Information Systems Frontiers, 19(3), 443-455.

Liu, J., Xiao, Y., Li, S., Liang, W., & Chen, C. P. (2012). Cyber security and privacy issues in smart grids. IEEE Communications Surveys & Tutorials, 14(4), 981-997.

Ma, Q., Schmidt, M. B., & Pearson, J. M. (2009). An Integrated Framework for Information Security Management. Review of Business, 30(1).

Majchrzak, A. (2004). Information security in cross-enterprise collaborative knowledge work. Information Security in Cross-Enterprise Collaborative Knowledge Work E: CO Issue, 6(4), 4-8.

Mandal, S. (2019). The influence of big data analytics management capabilities on supply chain preparedness, alertness and agility: An empirical investigation. Information Technology & People, 32(2), 297-318.

Marabelli, M., & Newell, S. (2012). Knowledge risks in organizational networks: The practice perspective. The Journal of Strategic Information Systems, 21(1), 18-30.

Martínez-Noya, A., & García-Canal, E. (2011). Technological capabilities and the decision to outsource/outsource offshore R&D services. International Business Review, 20(3), 264-277.

Mendelson, H. (2000). Organizational architecture and success in the information technology industry. Management Science, 46(4), 513-529.

Meng, G., Liu, Y., Zhang, J., Pokluda, A., & Boutaba, R. (2015). Collaborative security: A survey and taxonomy. ACM Computing Surveys (CSUR), 48(1), 1-38.

MOD, U. (2011). The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world.

Montoya-Torres, J. R., & Ortiz-Vargas, D. A. (2014). Collaboration and information sharing in dyadic supply chains: A literature review over the period 2000–2012. Estudios Gerenciales, 30(133), 343-354.

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. International Journal of Critical Infrastructure Protection, 3(3-4), 103-117.

Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2019). Cyber risk assessment and mitigation (CRAM) framework using logit and probit models for cyber insurance. Information Systems Frontiers, 21(5), 997-1018.

Murphy, Ian (2018). Cisco to train 120,000 cyber police. Retrieved from https://www.enterprisetimes.co.uk/2018/11/30/cisco-to-train-120000-cyber-police/ Accessed on December, 2020.

Naicker, V., & Mafaiti, M. (2019). The establishment of collaboration in managing information security through multisourcing. Computers & Security, 80, 224-237.

Naseer, H., Maynard, S. B., & Desouza, K. C. (2021). Demystifying analytical information processing capability: The case of cybersecurity incident response. Decision Support Systems, 143, 113476.

Ngo, L., Zhou, W., & Warren, M. (2005, September). Understanding transition towards information security culture change. AISM, 67-73.

Ortega-Ruiz, R., Del Rey, R., & Casas, J. A. (2012). Knowing, building and living together on internet and social networks: The ConRed cyberbullying prevention program. International Journal of Conflict and Violence (IJCV), 6(2), 302-312.

Osho, O., & Onoja, A. D. (2015). National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis. International Journal of Cyber Criminology, 9(1), 1-24.

Oviawe, J. I., Uwameiye, R., & Uddin, P. S. (2017). Bridging skill gap to meet technical, vocational education and training school-workplace collaboration in the 21st century. International Journal of vocational education and training research, 3(1), 7-14.

Papazafeiropoulou, A., & Spanaki, K. (2016). Understanding governance, risk and compliance information systems (GRC IS): The experts view. Information Systems Frontiers, 18(6), 1251-1263.

Parmigiani, A., & Mitchell, W. (2009). Complementarity, capabilities, and the boundaries of the firm: the impact of within-firm and interfirm expertise on concurrent sourcing of complementary components. Strategic Management Journal, 30(10), 1065-1091.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Computers & Security, 42, 165-176.

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.

Reay, I., Beatty, P., Dick, S., & Miller, J. (2013). Privacy policies and national culture on the internet. Information Systems Frontiers, 15(2), 279-292.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121-135.

Rothrock, R. A., Kaplan, J., & Van Der Oord, F. (2018). The board's role in managing cybersecurity risks. MIT Sloan Management Review, 59(2), 12-15

Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011, October). The role of cyber-security in information technology education. In Proceedings of the 2011 Conference on Information Technology Education. ACM, 113-122.

Safa, N. S., Maple, C., Watson, T., & Furnell, S. (2017). Information security collaboration formation in organisations. IET Information Security, 12(3), 238-245.

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. Journal of information security and applications, 40, 247-257.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. Computers & Security, 53, 65-78.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. computers & security, 56, 70-82.

Sampson, R. C. (2007). R&D alliances and firm performance: The impact of technological diversity and alliance organization on innovation. Academy of management journal, 50(2), 364-386.

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.

Schlienger, T., & Teufel, S. (2003). Information security culture-from analysis to change. South African Computer Journal, 2003(31), 46-52.

Sedera, D., & Gable, G. G. (2010). Knowledge management competence for enterprise system success. The Journal of Strategic Information Systems, 19(4), 296-306.

Sharma, D., Taggar, R., Bindra, S. and Dhir, S. (2020a), “A systematic review of responsiveness to develop future research agenda: a TCCM and bibliometric analysis”, Benchmarking: An International Journal, Vol. 27 No. 9, pp. 2649-2677.

Sharma, D., Taggar, R., Bindra, S. and Dhir, S. (2020b), “Retailer responsiveness: a total interpretive structural modelling approach”, Journal for Global Business Advancement, Vol. 13 No. 3, pp. 336-358.

Sheng, S., Chan, W. L., Li, K. K., Xianzhong, D., & Xiangjun, Z. (2007). Context information-based cyber security defense of protection system. IEEE Transactions on Power Delivery, 22(3), 1477-1481.

Shollo, A., Constantiou, I., & Kreiner, K. (2015). The interplay between evidence and judgment in the IT project prioritization process. The Journal of Strategic Information Systems, 24(3), 171-188.

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of “organizational information security management”. Journal of Enterprise Information Management.

Singhal, M., Chandrasekhar, S., Ge, T., Sandhu, R., Krishnan, R., Ahn, G. J., & Bertino, E. (2013). Collaboration in multicloud computing environments: Framework and security issues. Computer, 46(2), 76-84.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), 31-41.

Smith, G. E., Watson, K. J., Baker, W. H., & Pokorski Ii, J. A. (2007). A critical balance: collaboration and security in the IT-enabled supply chain. International Journal of Production Research, 45(11), 2595-2613.

Sohrabi Safa, N., Maple, C., Watson, T., & Furnell, S. (2018). Information security collaboration formation in organisations. IET Information Security, 12(3), 238-245.

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

Sousa, M. J., & González-Loureiro, M. (2016). Employee knowledge profiles–a mixed-research methods approach. Information Systems Frontiers, 18(6), 1103-1117.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. Future Generation Computer Systems, 92, 178-188.

Srivastava, A. K., & Sushil. (2013). Modeling strategic performance factors for effective strategy execution. International Journal of Productivity and Performance Management, 62(6), 554-582.

Srivastava, M. K., Gnyawali, D. R., & Hatfield, D. E. (2015). Behavioral implications of absorptive capacity: The role of technological effort and technological capability in leveraging alliance network technological resources. Technological Forecasting and Social Change, 92, 346-358.

Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. Information & Computer Security.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. MIS Quarterly, 441-469.

Stuart, T. E. (2000). Interorganizational alliances and the performance of firms: a study of growth and innovation rates in a high-technology industry. Strategic management journal, 21(8), 791-811.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11.

Summers, R. F., & Barber, J. P. (2003). Therapeutic alliance as a measurable psychotherapy skill. Academic Psychiatry, 27(3), 160-165.

Sushil, A. (2017a). Modified ISM/TISM process with simultaneous transitivity checks for reduced direct pair comparisons. Global Journal of Flexible Systems Management, 18(4), 331-351.

Sushil, S. (2012). Interpreting the interpretive structural model. Global Journal of Flexible Systems Management, 13(2), 87-106.

Sushil. (2017b). Multi-criteria valuation of flexibility initiatives using integrated TISM–IRP with a big data framework. Production Planning & Control, 28(11-12), 999-1010.

Sushil. (2018a). How to check correctness of total interpretive structural models?. Annals of Operations Research, 270(2), 473-487.

Sushil. (2018b). Incorporating polarity of relationships in ISM and TISM for theory building in information and organization management. International Journal of Information Management, 43(1), 38-51.

Switzer, L. N., & Wang, J. (2017). An event based approach for quantifying the effects of securities fraud in the IT industry. Information Systems Frontiers, 19(3), 457-467.

Talja, S. (2002). Information sharing in academic communities: Types and levels of collaboration in information seeking and use. New Review of Information Behavior Research, 3(1), 143-159.

Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. Behaviour & Information Technology, 32(10), 1014-1023.

Trkman, P., & Desouza, K. C. (2012). Knowledge risks in organizational networks: An exploratory framework. The Journal of Strategic Information Systems, 21(1), 1-17.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. European Journal of Information Systems, 24(1), 38-58.

Valentine, J. A. (2006). Enhancing the employee security awareness model. Computer Fraud & Security, 2006(6), 17-19.

Venkatraman, N., Henderson, J. C., & Oldach, S. (1993). Continuous strategic alignment: Exploiting information technology capabilities for competitive success. European Management Journal, 11(2), 139-149.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102.

Wang, S., & Wang, H. (2019). Knowledge Management for Cybersecurity in Business Organizations: A Case Study. Journal of Computer Information Systems, 1-8.

Warfield, J. N. (1974). Toward interpretation of complex structural models. IEEE Transactions on Systems, Man, and Cybernetics, 5(1), 405-417.

Wasuja, S., Sagar, M., & Sushil. (2012). Cognitive bias in salespersons in specialty drug selling of pharmaceutical industry. International Journal of Pharmaceutical and Healthcare Marketing, 6(4), 310-335.

Wedutenko, A. (2015). Cyber attacks: Get your governance in order. Governance Directions, 67(10), 598.

Westin, A. F. (1966). Science, privacy, and freedom: Issues and proposals for the 1970's. Part I--The current impact of surveillance on privacy. Columbia Law Review, 66(6), 1003-1050.

Westrum, R. (2004). A typology of organisational cultures. Quality and Safety in Health Care, 13(2), 22–27.

Westrum, R. (2014). The study of information flow: A personal journey. Safety Science, 67(1), 58-63.

White, J. (2016). Cyber Threats and Cyber Security: National Security Issues, Policy and Strategies. Global Security Studies, 7(4).

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. Computers & Security, 88, 101640.

Yadav, N., S., & Sagar, M. (2015). Modeling strategic performance management of automobile manufacturing enterprises: an Indian context. Journal of Modelling in Management, 10(2), 198-225.

Yazici, H. J. (2002). The role of communication in organizational change: An empirical investigation. Information & Management, 39(7), 539-552.

Zafar, H., Ko, M. S., & Osei-Bryson, K. M. (2016). The value of the CIO in the top management team on performance in the case of information security breaches. Information Systems Frontiers, 18(6), 1205-1215.

Zammuto, R. F., Griffith, T. L., Majchrzak, A., Dougherty, D. J., & Faraj, S. (2007). Information technology and the changing fabric of organization. Organization Science, 18(5), 749-762.

Zhang, X., Tsang, A., Yue, W. T., & Chau, M. (2015). The classification of hackers by knowledge exchange behaviors. Information Systems Frontiers, 17(6), 1239-1251.

Zuo, Y., & O'Keefe, T. (2007). Post-release information privacy protection: A framework and next-generation privacy-enhanced operating system. Information Systems Frontiers, 9(5), 451-467.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: a comparative study. Journal of Computer Information Systems, 1-16.

Table 1 Identified factors

SN	Factor	Factor Code	Supporting Literature
1	Resources and Capabilities	C1	Klaic and Ph, 2015; Saunila et al., 2019
2	Information Flow	C2	Akella et al., 2010; Sheng et al., 2007
3	Training	C3	Berry and Berry, 2018; Bodeau and Graubart, 2016; Dodge et al., 2003
4	Alliance and Collaboration	C4	Ključnikov, Mura and Sklenár, 2019; Rowe et al., 2011; Talja, 2002; Cains et al., 2021
5	Governance	C5	Bodeau and Graubart, 2016; Ključnikov, Mura and Sklenár 2019; Zafar, Ko and Osei-Bryson, 2016
6	Security Awareness	C6	Kritzinger and Von Solms, 2010; Li et al., 2019; Wiley, McCormac, and Calic, 2020
7	Technological Infrastructure	C7	Byres and Hoffman, 2004; Klaic and Ph, 2015

Table 2 Contextual relationship and interpretation for the factors of cybersecurity

Factor Code	Factor Name	Contextual relationship	Interpretation
C1	Resources and capabilities	Factor A will influence/ enhance Factor B	How or in what way a Factor A will influence/enhance Factor B?
C2	Information flow		
C3	Training		
C4	Alliance and Collaboration		
C5	Governance		
C6	Security awareness		
C7	Technological Infrastructure		

Table 3 Reachability matrix with transitivity

Elements	C1	C2	C3	C4	C5	C6	C7
C1	1	1	0	0	0	1*	1

C2	0	1	0	0	0	1	0
C3	0	1	1	0	0	1*	0
C4	1	1*	1	1	0	1*	1*
C5	1*	1*	1*	1	1	1	1*
C6	0	1	0	0	0	1	0
C7	0	0	0	0	0	0	1

*Transitive links

Table 4 Partitioning the reachability matrix into different levels

Elements	**Reachability Set**	**Antecedent Set**	**Intersection Set**	**Level**
(a): Iteration-1				
C1	1,2,6,7	1,4,5	1	
C2	2,6	1,2,3,4,5,6	2,6	**I**
C3	2,3,6	3,4,5	3	
C4	1,2,3,4,6,7	4,5	4	
C5	1,2,3,4,5,6,7	5	5	
C6	2,6	1,2,3,4,5,6	2,6	**I**
C7	7	1,4,5,7	7	**I**
(b): Iteration-2				
C1	1	1,4,5	1	**II**
C3	3	3,4,5	3	**II**
C4	1,3,4	4,5	4	
C5	1,3,4,5	5	5	
(c): Iteration-3				
C4	4	4,5	4	**III**
C5	4,5	5	5	
(d): Iteration-4				
C5	5	5	5	**IV**

Table 5 Factors and their levels to build M-TISM model

SN	**Factor Code**	**Factor Name**	**Level in M-TISM**
1	C2	Information flow	I
2	C6	Security awareness	I
3	C7	Technological Infrastructure	I
4	C1	Resources and capabilities	II
5	C3	Training	II
6	C4	Alliance and collaboration	III
7	C5	Governance	IV

Table 6 Binary matrix

Element	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**
C1	-	1	0	0	0	0	1
C2	0	-	0	0	0	1	0
C3	0	1	-	0	0	1	0
C4	1	1	1	-	0	0	1
C5	0	0	0	1	-	0	0
C6	0	1	0	0	0	-	0
C7	0	0	0	0	0	0	-

Table 7: Interpretive logic - Knowledge Base

SN	Element codes	Pairwise comparison	Interpretation	Supporting literature
1	C1-C2	Resources and capabilities will enhance the information flow	The organization will achieve information security and smooth flow of information	Arden et al., 2012; Kwon and Johnson, 2012
2	C4-C1	The alliance and collaboration will enhance resources and capabilities	Alliances bring complementary resources and facilitate the flow of knowledge resulting in higher security performance	Chang, 2004; Gulati, 1999; Ključnikov, Mura and Sklenár, 2019; Safa et al., 2018
5	C1-C7	Resources and capabilities will enhance the Technological Infrastructure	Significant resources secure cyberspace by using a combination of technologies, software, and systems	Kwon and Johnson, 2012; Rhee et al., 2009
6	C3-C2	Training will enhance the information flow	Knowledge and training programs develop the skill of employees and enhance the flow of information	Berry and Berry, 2018; Hota et al., 2015; Hou et al., 2018; Ruighaver et al., 2007
7	C4-C2	Transitive	The alliance could raise the knowledge and experience of the workforce within firms	Hou et al., 2018; Knox, 2018; Safa et al., 2018
9	C2-C6	Information flow will enhance security awareness	Improves the functionality and provides awareness of unauthorized access and improper handling of unwanted documents	Kim and Jeoung, 2015; Kim and Solomon, 2012; Li et al., 2019
10	C6-C2	Security awareness will enhance information flow	Increases the level of consciousness sharing of sensitive information	Dahbur et al., 2017; Li et al., 2019; Stewart et al., 2015
11	C4-C3	The alliance and collaboration will enhance knowledge and training	Collaboration or alliance could raise the knowledge and experience of the workforce within firms, which can result in the development of new knowledge and skills	Ključnikov, Mura and Sklenár, 2019; Santoro et al., 2006; Yang and Chen, 2008
13	C3-C6	Transitive	Develops employee’s knowledge and skills, increase awareness of employees, and improves information security management	Crossler et al., 2012; Ruighaver et al., 2007; Wiley, McCormac, and Calic, 2020
14	C5-C4	Governance will enhance alliance and collaboration	Successful collaboration will enhance cybersecurity strategy through sharing knowledge and resources, which requires full engagement from the senior management team	de Bruijn and Janssen, 2017; Franke and Brynielsson, 2014; Ključnikov, Mura and Sklenár, 2019
16	C4-C7	Transitive	Alliance through the sharing of security allied data and technologies will develop and update the current infrastructure of software and tools required	Cotugna and Vickery, 2003; Safa et al., 2018; Sanders, 2007

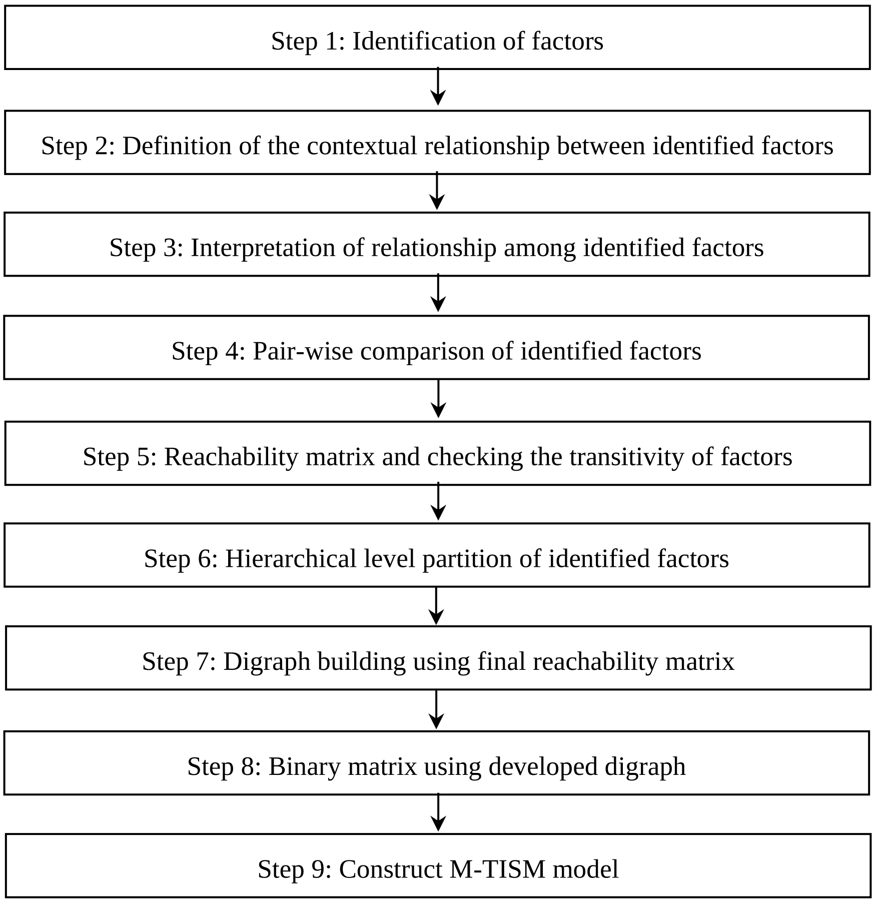
Step 1: Identification of factors
Step 2: Definition of the contextual relationship between identified factors
Step 3: Interpretation of relationship among identified factors
Step 4: Pair-wise comparison of identified factors
Step 5: Reachability matrix and checking the transitivity of factors
Step 6: Hierarchical level partition of identified factors
Step 7: Digraph building using final reachability matrix
Step 8: Binary matrix using developed digraph
Step 9: Construct M-TISM model

Fig. 1. M-TISM process

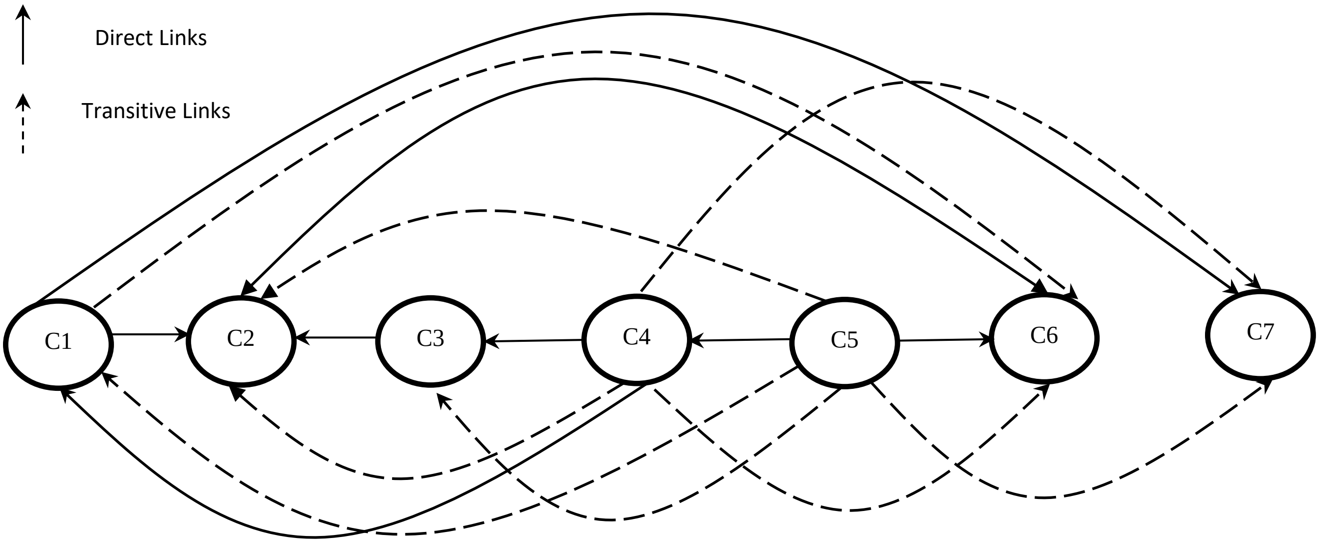

Fig. 2. Successive comparison digraph as per M-TISM process

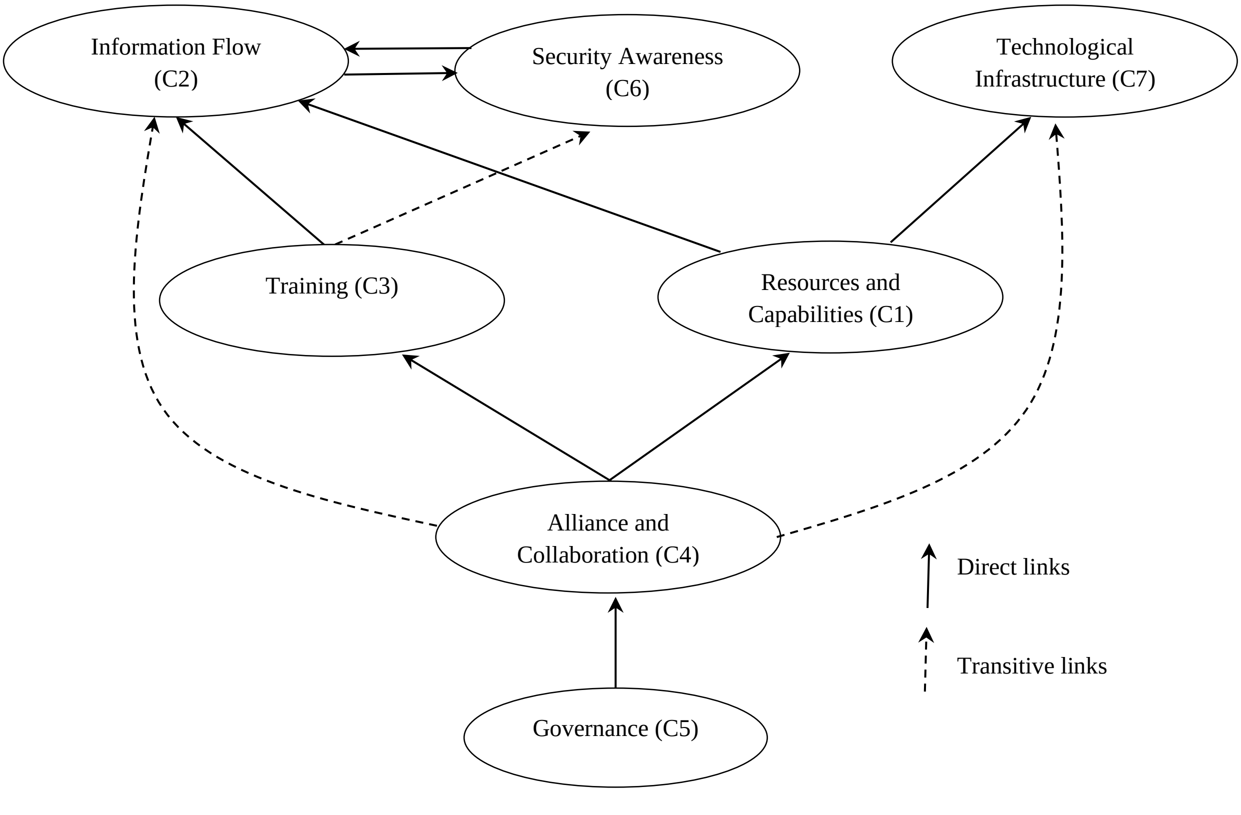

Fig. 3. ISM Digraph after hierarchical partitioning of factors

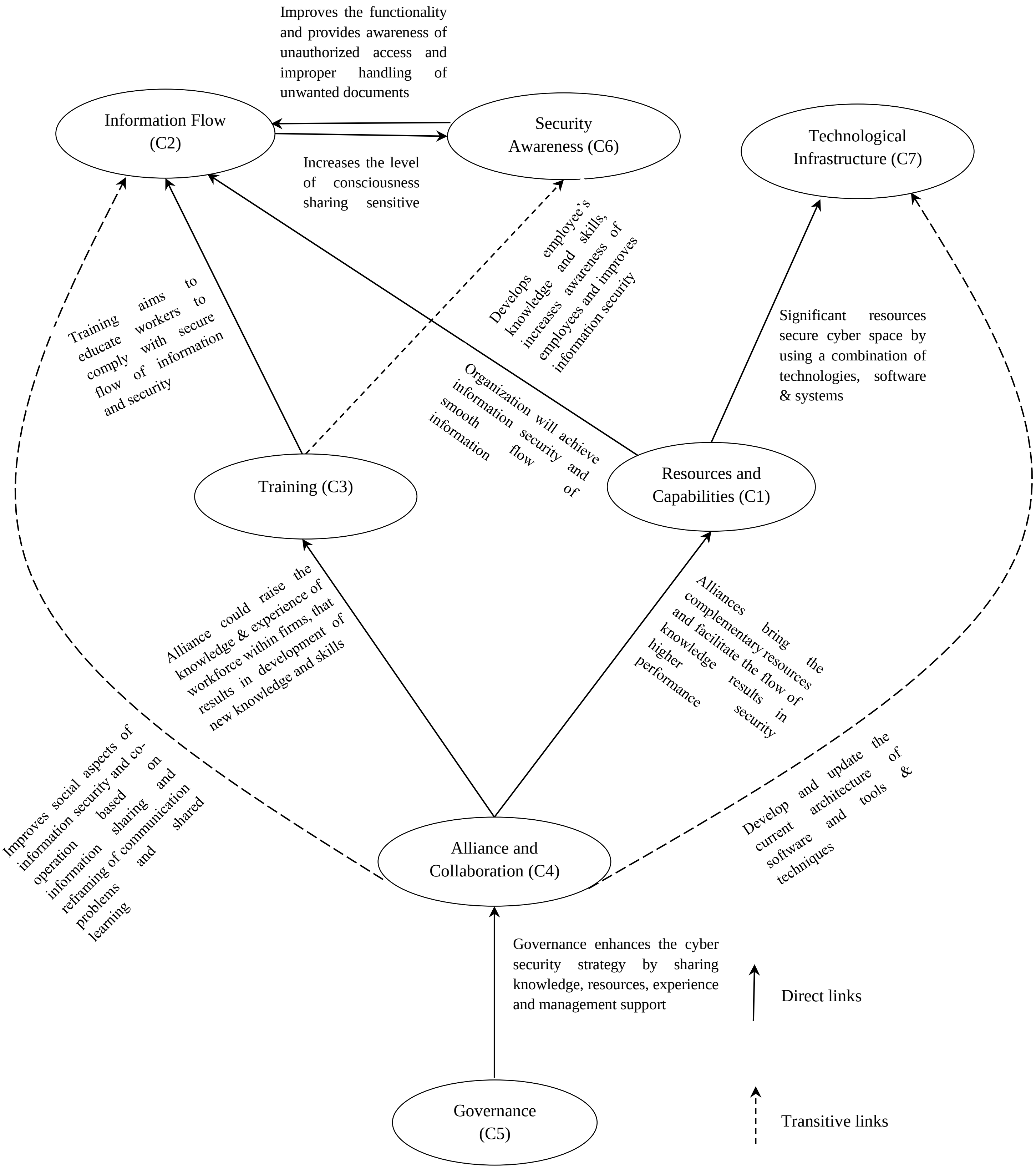
Improves the functionality and provides awareness of unauthorized access and improper handling of unwanted documents
Information Flow (C2)
Security Awareness (C6)
Technological Infrastructure (C7)
Increases the level of consciousness sharing sensitive
Develops employee's knowledge and skills, increases awareness of employees and improves information security
Training aims to educate workers to comply with secure flow of information and security
Significant resources secure cyber space by using a combination of technologies, software & systems
Organization will achieve information security and smooth flow of information
Training (C3)
Resources and Capabilities (C1)
Alliance could raise the knowledge & experience of workforce within firms, that results in development of new knowledge and skills
Alliances bring the complementary resources and facilitate the flow of knowledge results in higher security performance
Improves social aspects of information security and co-operation based on information sharing and reframing of communication problems and shared learning
Develop and update the current architecture of software and tools & techniques
Alliance and Collaboration (C4)
Governance enhances the cyber security strategy by sharing knowledge, resources, experience and management support
Direct links
Transitive links
Governance (C5)

Fig. 4. M-TISM Model

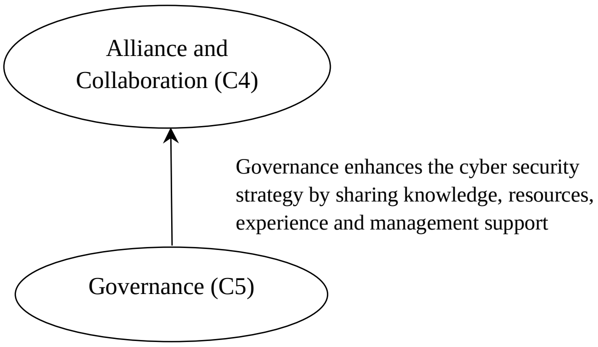
Alliance and Collaboration (C4)
Governance enhances the cyber security strategy by sharing knowledge, resources, experience and management support
Governance (C5)

Fig. 5. Validation and justification of Path 1 of the M-TISM model

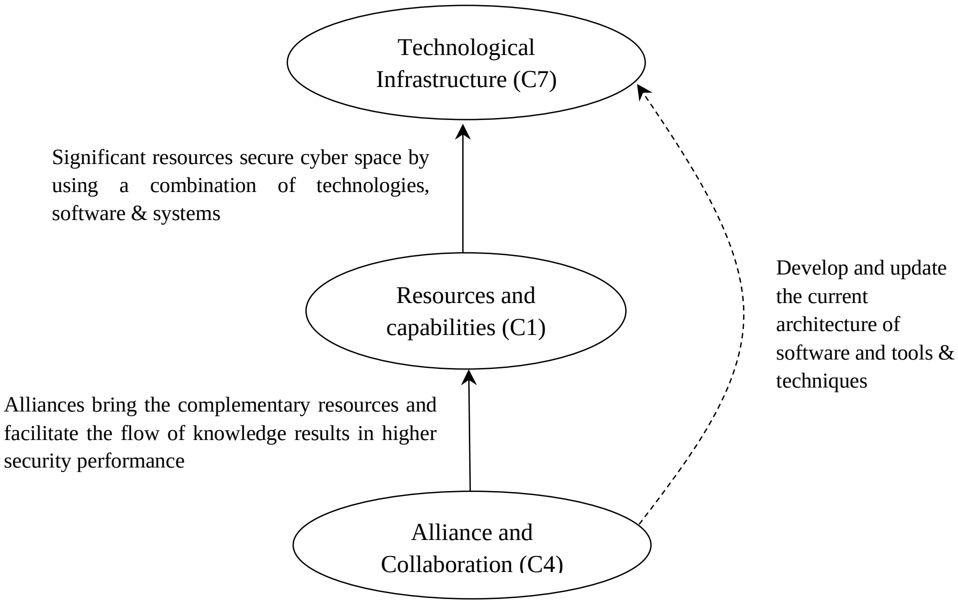
Technological Infrastructure (C7)
Significant resources secure cyber space by using a combination of technologies, software & systems
Develop and update the current architecture of software and tools & techniques
Resources and capabilities (C1)
Alliances bring the complementary resources and facilitate the flow of knowledge results in higher security performance
Alliance and Collaboration (C4)

Fig. 6. Validation and justification of Path 2 of the M-TISM model

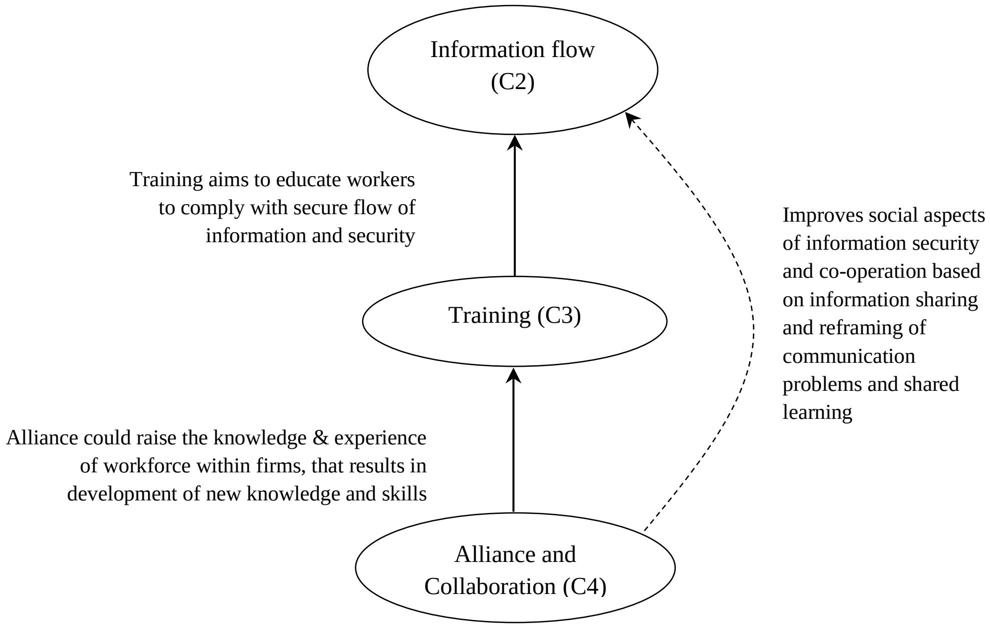
Information flow (C2)
Training aims to educate workers to comply with secure flow of information and security
Improves social aspects of information security and co-operation based on information sharing and reframing of communication problems and shared learning
Training (C3)
Alliance could raise the knowledge & experience of workforce within firms, that results in development of new knowledge and skills
Alliance and Collaboration (C4)

Fig. 7. Validation and justification of Path 3 of the M-TISM model

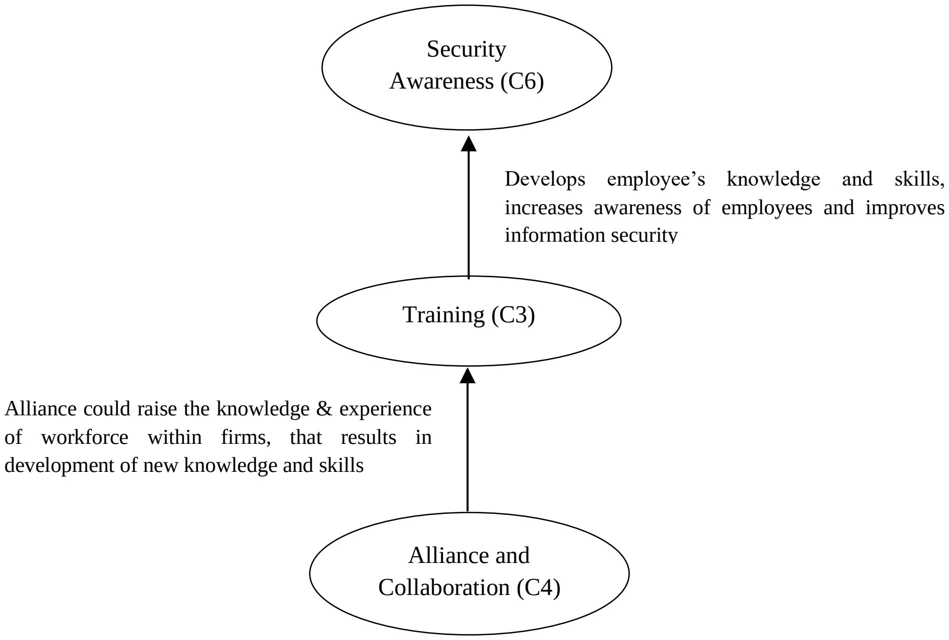
Security Awareness (C6)
Develops employee's knowledge and skills, increases awareness of employees and improves information security
Training (C3)
Alliance could raise the knowledge & experience of workforce within firms, that results in development of new knowledge and skills
Alliance and Collaboration (C4)

Fig. 8 Validation and justification of Path 4 of the M-TISM model

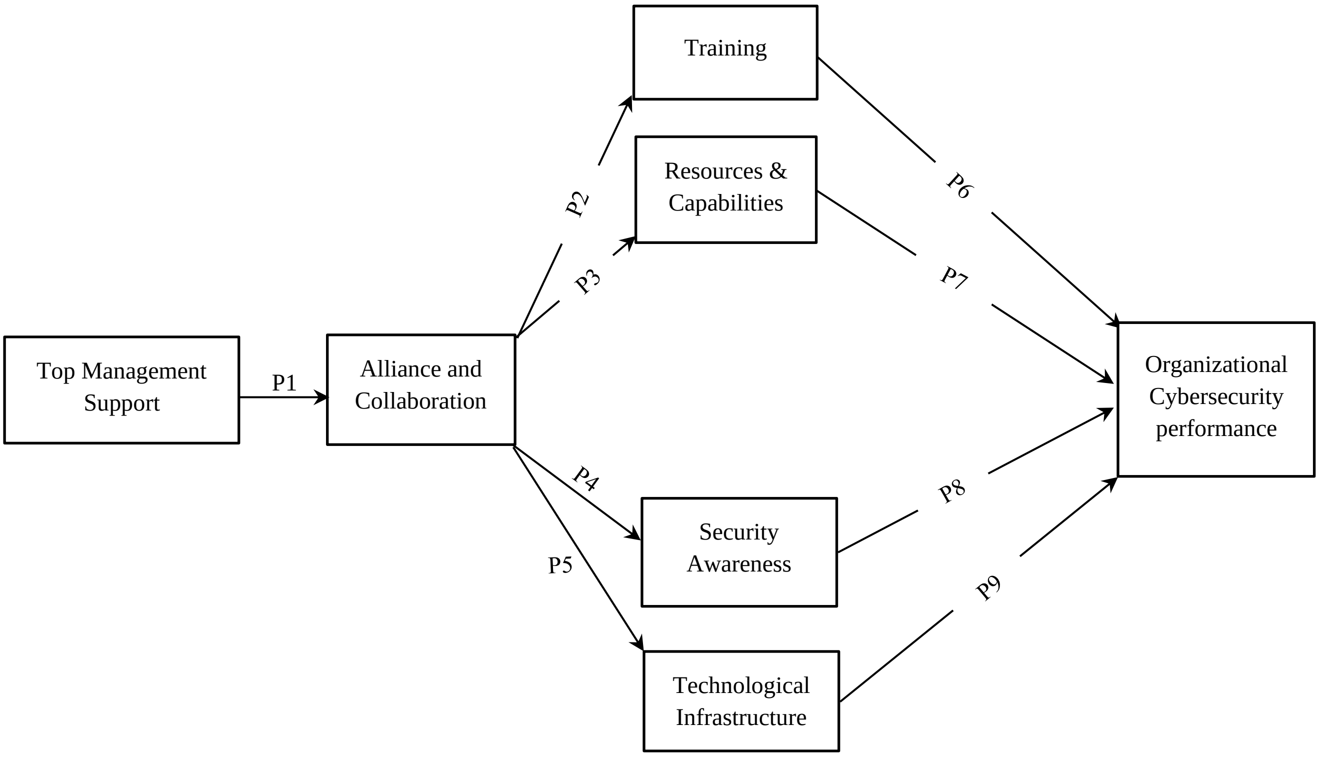
Training
Resources & Capabilities
Top Management Support
P1
Alliance and Collaboration
P2
P3
P4
P5
Security Awareness
Technological Infrastructure
P6
P7
P8
P9
Organizational Cybersecurity performance

Fig. 9 Proposed model for the cybersecurity management