

## A model for information security culture with creativity and innovation as enablers - refined with an expert panel

Adéle da Veiga <sup>[0000-0001-9777-8721]</sup>

School of Computing, College of Science, Engineering and Technology, University of South Africa (UNISA), Florida, Johannesburg, South Africa  
dveiga@unisa.ac.za

**Purpose:** This research aims to elicit an understanding of creativity and innovation to enable a totally aligned information security culture. A model is proposed to encourage creativity and innovation as part of the information security culture.

**Design/methodology/approach:** The study firstly applied a theoretical approach with a scoping literature review using the PRISMA method to propose a conceptual model for engendering employee creativity and innovation as part of the information security culture. A qualitative research method was further applied with expert interviews and qualitative data analysis in Atlas.ti to validate and refine the conceptual model.

**Findings:** A refined and validated information security culture model enabled through creativity and innovation (ISC-C&I) is presented. The input from the expert panel was used to extend the model by 18 elements highlighting that the risk appetite of an organisation defines how much creativity and innovation can be tolerated in order to reach a balance with the potential risks it might introduce. Embedding creativity and innovation as part of the organisational culture to facilitate it further as part of the information security culture can aid in combating cyber threats and incidents; however, it should be managed through a decision-making process while governed within policies that define the boundaries of creativity and innovation in information security.

**Originality:** The research proposes a novel concept of introducing creativity and innovation as part of the information security culture and presents a novel model to facilitate this.

**Research limitations/implications:** The research serves as a point of reference for further research about the influence of creativity and innovation in information security culture which can be investigated through structural equation modelling.

**Practical implications:** This study offers novel insights for managerial practice to encourage creativity and innovation as part of information security.

**Keywords:** information security culture, information security, creativity, innovation, model, organisational culture

### 1 Introduction

Creativity is critical to organisational success (Andleeb, Ahmad, Hassan, Rahman, Abdullah and Nawi, 2020) while innovation is regarded as a driver for organisational growth, resilience (Javanmardi, Wiewiora and Mohannak, 2021), sustainability (Robbins, Judge, Odendaal and Roodt, 2018), performance (Strychalska-Rudzewicz and Rudzewicz, 2021), and competitiveness (Bianchi, Tontini and Gomes, 2021). Creativity and innovation are becoming a core part of organisational strategies to achieve success and to incorporate technology changes (Shahzad, Xiu and Shahbaz, 2017) these being key factors that can aid organisations to adapt in a world where there is an accelerated pace of change (Martins and Terblanche, 2003). Creativity and innovation will play a critical role in equipping organisations to become cyber resilient, to manage through the change brought about by the fourth industrial revolution (Makumbe, 2021), and to enhance organisational effectiveness by also applying innovation in information systems security (Hwang and Choi, 2017). Research has shown that 88% of board members are

concerned about cyber threats (Mimecast, 2022), affecting the confidentiality, integrity, and availability of information and information systems. With increasing numbers of cyberattacks and data breaches, organisations need to be creative and innovative if they are to combat threats and become cyber resilient. The human element is still a key target in attacks and often part of the threat (ENISA, 2017; Da Veiga, Astakhova, Botha and Herselman, 2020). Phishing attacks accounted for most data breaches in 2021, with 96% occurring via e-mails targeting end-users (Mimecast, 2022). Information security challenges, especially those related to end-users, require organisations to develop an information security culture where creativity and innovation are encouraged to protect information and information systems.

Organisational culture is seen as an enabler to facilitate creativity and innovation in an organisation (Bianchi *et al.*, 2021; Javanmardi Kashan *et al.*, 2021; Martins and Terblanche, 2003; Scaliza, Jugend, Chiappetta Jabbour, Latan, Armellini, Twigg and Andrade, 2022). Organisational culture can be explained as the assumptions, beliefs, values, and norms that are shared by employees (Schein, 1985) and that distinguish the organisation from other organisations (Robbins *et al.*, 2018). Values, beliefs, and knowledge of employees influence the organisational culture, but they also shape the employee's cognition, motivation, and problem-solving (Lin and Wittmer, 2017) that are visible in the employee behaviour. This behaviour of employees should be shaped to be in line with the organisation's information security policies where compliance behaviour is required. In an organisation where there is a supportive organisational culture for creativity and innovation, employees will be equipped to solve information security issues and problems (Lin and Wittmer, 2017). Creativity on the part of individual employees extends to problem-solving and competency in information security and individuals require such to address security issues that occur in their daily work (Lin and Wittmer, 2017). Innovation and creativity could therefore play an additional role in aiding with problem-solving to combat cyberattacks and data breaches and to encourage employee behaviour that mitigates risks to information protection.

Information security culture research has shown that a strong information security culture can aid in protecting information and in minimising employee behaviour that results in information security risk or data breaches (ENISA, 2017; Tolah, Furnell and Papadaki, 2021; Da Veiga *et al.*, 2020). The factors that influence information security culture have been defined and investigated in numerous studies (AlHogail, 2015; Tolah *et al.*, 2021; Da Veiga *et al.*, 2020). To date, however, there has not been a study that has considered creativity and innovation to strengthen the information security culture. Nonetheless, numerous research studies have been conducted about the role of creativity and innovation in an organisational culture (Andleeb *et al.*, 2020; Bianchi *et al.*, 2021; Javanmardi Kashan *et al.*, 2021; Martins, Martins and Terblanche, 2004) and these studies can be leveraged in an information security context.

The objective of this paper is to propose a model whereby creativity and innovation are applied to strengthen an information security culture. This study is conducted by applying a scoping literature review and building on research in the organisational culture domain whereafter the model is validated and refined with expert interviews. The research question that has guided this research is, "What would an information security culture model comprise where innovation and creativity are used as enablers?"

## **2 Background**

### **2.1 Information security culture**

An information security culture is a subculture of the organisational culture (Hayden, 2016; Niekerk and Solms, 2005; Schlienger and Teufel, 2002). In line with Schein's (1985) definition of organisational culture, the information security culture also comprises assumptions, values, beliefs, and attitudes (Schlienger and Teufel, 2002; von Solms and van Niekerk, 2013) of employees toward information security. These influence the employee behaviour when employees interact with information and information systems and, over time, become the way things are done in the organisation to protect information and information systems and will be visible in behaviour and artifacts in the organisation (Da Veiga, 2019, 2021). It is critical that the way things are done in an organisation is in line with the information security policy of the organisation and that employees share the same values and beliefs to protect information. In order to secure and protect information effectively, a strong information security culture is required (ENISA, 2017). The organisation should aim for a totally aligned information security culture where the strategy of the organisation, as well as employee behaviour and values, are both in support of the protection of information (Da Veiga, 2019). A strong information security culture will enable positive employee behaviour, thereby leading to fewer security incidents and data breaches arising from end-user threats due to errors or negligent behaviour (Da Veiga, 2019). Information security should be part of the organisational strategy and vision and should be seen as a

strategic advantage, as opposed to a hindrance. In an organisational culture where information security is valued, one would observe compliant behaviour which is strengthened through positive reinforcement and proactive interventions such as awareness, education and training of employees.

## 2.2 Creativity and innovation in an organisation

The terms “creativity” and “innovation” are used interchangeably and together in literature (Auernhammer and Hall, 2014; Martins *et al.*, 2004). Creativity is part of the innovation processes, with innovation resulting after creativity (Cuicui, Mateescu and Cuicui, 2014; Shahzad, Xiu and Shahbaz, 2017) as part of a routine process. Creativity is seen by some researchers as a subset of innovation (Scheibe and Gupta, 2017) whereby new ways to resolve a problem are expected. Creativity is regarded as a requirement for innovation; however, authors agree that creativity does not always result in innovation (Scheibe and Gupta, 2017). Willingness and creativity (which relate to intrinsic motivation) lead to the generation of new ideas, resulting in turn in knowledge creation when applied in a work situation (Auernhammer and Hall, 2014). To encourage innovation in an organisation, a bottom-up approach can be followed, with ideas emanating from employees, or a top-down approach can be taken, with the organisation driving creativity through its vision and strategy (Cuicui *et al.*, 2014). Creativity in an organisation can also be achieved by encouraging creativity in individual employees in three areas, namely, “expertise, creative thinking skills and intrinsic task motivation” (Robbins *et al.*, 2018). Creative ideas from individuals and groups lead to new approaches, solutions (Ogbeibu, Senadjki and Luen Peng, 2018) and problem-solving. These, as part of a dynamic process in an organisation, will result in knowledge creation. The organisational culture can be conducive to creativity and innovation or hinder them. In either case, there is an impact on creativity and innovation through basic values, assumptions, and beliefs which are translated into artifacts such as the information security policy and management processes (Martins and Terblanche, 2003). When management provides employees with resources to develop new ideas or to solve problems, they will perceive it as valuable, which will influence how they behave (Martins and Terblanche, 2003).

## 2.3 Applying creativity and innovation in information security culture

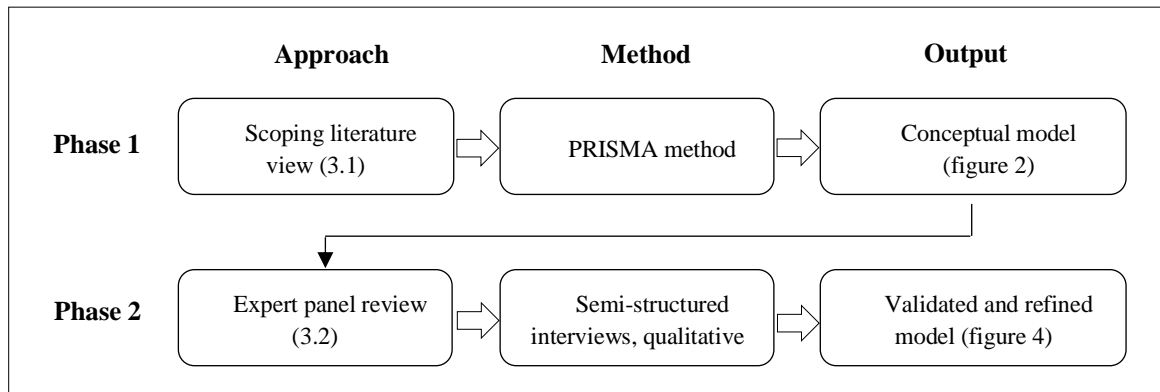
An information security culture is required where innovation for information security is supported and where the employees of the organisation feel encouraged to support information security but also to partake in the day-to-day implementation thereof (Hwang and Choi, 2017). Employees of an organisation will be more committed to innovation in information security, as well as more committed to implementing and upholding it, in an organisational culture where flexibility is promoted and where such organisational culture is conducive to information system security innovation (Hwang and Choi, 2017). One of the cultures that are found to be supportive of innovation in information security is the open culture, where employees are seen as flexible with a focus on the future (Hwang and Choi, 2017). Hwang and Choi state, for “or ISS to be effective, a culture that facilitates information security and supports ISS innovation is crucial for encouraging members to support ISS and actively participate in its implementation” (Hwang and Choi, 2017: 187). The behaviour of each employee in the organisation impacts on the effectiveness of information security, which means that their behaviour should be in line with the policies, standards, procedures, and required practices of the organisation, as directed by the organisation’s management and leadership (Hwang and Choi, 2017). In the study by Hwang and Choi (2017), it is argued that there is an incumbency on every employee to implement information system security policies in order for information system security to be effective. However, they also emphasise that there should be a culture in the organisation that supports information system security innovation, as promoted by the leaders of the organisation, in order for the employees to adopt the culture and for their own values and beliefs to be aligned to that culture. There is, however, no guidance on how management should foster an information security culture that is enabled through creativity and innovation.

## 3 Research methodology

The research methodology followed a phased approach as illustrated in figure 1 whereby phase one comprised of a scoping literature review that was conducted using the PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses) method to develop the conceptual model which was published as part of the conceptual study (Da Veiga 2022) and is presented in figure 2. This was followed by phase 2 to validate and refine the conceptual

model with an expert panel using semi-structured interviews and qualitative data analysis as part of the research method. The final output is the validated and refined information security culture model with creativity and innovation as enablers (ISC-C&I Model) and is presented in figure 4.

**Figure 1:** Phased research approach



### 3.1 Phase 1: Scoping literature review

The literature review study was conducted using a scoping literature review approach to identify the extent of research published focusing on creativity and innovation in an information security culture context (Grant, Booth and Centre, 2009). The PRISMA method was applied to gather, screen, and review the retrieved research papers systematically (Moher, Liberati, Tetzlaff, Altman and Group, 2009).

#### 3.1.1 Method

Two literature searches were conducted in the Emerald, Science Direct, Scopus, and Web of Science databases. The first search used the keywords: (title: Information security culture) AND (abstract: Innovation OR Creativity) in the abstract, between the years 2011 and 2022, and in English. Only two papers from Web of Science, (Hwang and Choi, 2017; Lin and Wittmer, 2017) were extracted. Due to the limited research previously carried out on creativity and innovation in information security culture, a second literature search was conducted to identify studies where creativity and innovation were considered as part of organisational culture. Table 1 outlines the results of the second literature search. A total of 18 papers were included in the full-text review. The next section provides a summary of the eligible papers.

**Table 1:** PRISMA approach for literature search

Databases	(Title: “organisational culture”) AND (title Innovation OR Creativity) in abstract, 2011-2022, English				
	#Records identified through database searching	#Records after duplicates removed	#Records screened	#Records excluded (exclusion/inclusion criteria)	#Full-text articles assessed for eligibility
Emerald	1	1	1	0	1
Science Direct	6	6	6	1	5
Scopus	21	21	21	15	6
WoS	18	17	17	11	6

#### 3.1.2 Results

##### 3.1.2.1 Creativity and innovation in the information security culture context

Hwang and Choi (2017) conducted a study in the e-government sector to investigate innovation in information systems security. They argued that increased organisational effectiveness can be established if there is a culture for

information systems security innovation. The participating organisation fostered an information systems security innovative-support culture, which incorporated an information security culture. Some of the key factors focused on to facilitate this were formal and informal communication and education, as well as training programmes on the organisational, group, and interpersonal levels. They also introduced an artifact creation programme to aid in shifting security attitudes to information systems. They used the example of symbols or mottos about information systems security aspects which can be shown on end-users' computer screens.

Individual creativity was emphasised as an important factor to facilitate problem-solving concerned with information security issues at work (Lin and Wittmer, 2017). The authors refer to the work of Ambile (1996) in which creativity is portrayed as task motivation, domain-relevant skills, and creativity-relevant processes. Task motivation relates to intrinsic (internally motivated, "inherently interesting or enjoyable" (Padayachee, 2012)) as well as extrinsic motivation (such as rewards for compliance, leading to an outcome (Padayachee, 2012)). Intrinsic motivation is linked with commitment, which, in turn, is associated with task completion at work and can assist in the completion of information security tasks and problem-solving. The implementation of security awareness and training in organisations assists in developing the domain-relevant skills that are necessary for employees to apply in their work. These skills are a prerequisite to facilitating creativity in information security problem-solving. This supports research that showed if employees are trained, they are five times more likely to identify and avoid clicking on malicious links (Mimecast, 2022). Lin and Wittmer (2017) argued that creativity-relevant processes, which are the manner or pathways in which a solution is derived, are required for problem-solving in information security management.

### 3.1.2.2 Creativity and innovation in an organisational culture context

Martins and Meyer (2012) conducted a study to investigate aspects of organisational culture and behaviour that influence knowledge retention in an organisation. The paper refers to creativity, but not in the context of an innovation culture. Earlier work of Martins (Martins *et al.*, 2004; Martins and Terblanche, 2003) focused on the development of a model for the Influence of Organisational Culture on Creativity and Innovation, using determinants of organisational culture that promote creativity and innovation, these being: strategy of the organisation, with a vision and mission that support creativity and innovation; purposefulness (vision and mission understanding); trust relationships (trust and support for change); behaviour that encourages innovation (idea-generation, risk-taking, decision-making); working environment (goals and objectives, conflict handling, cooperative teams, participation, control of own work); customer orientation (flexibility and improvement in service, understanding needs); and management support (open communication, availability of resources, tolerance of mistakes, adaption of rules and regulations).

Other aspects that support creativity and innovation in an organisation are the organisational structure being non-hierarchical, autonomy, working in teams, freedom, being flexible; support mechanisms (e.g., rewards and recognition, use of technology, recruitment of certain types of employees valuing diversity, energetic, with knowledge, inquisitiveness); behaviour (e.g., tolerance of mistakes, taking risks and experimenting, as long as it does not harm the organisation, support for change); and communication (open and transparent) (Martins and Terblanche, 2003). The study by Martins *et al.* (2004) did not focus on what type of organisational culture promotes creativity and innovation, but rather defined the elements that could determine or encourage creativity and innovation as part of an organisational culture.

The Competing Values Framework of Cameron and Quinn (2011) and Quinn and Rohrbaugh (1983) is used to measure organisational culture in four distinct quadrants, namely, Hierarchy, Market (Rational), Clan (Group), or Adhocracy (Developmental) through the evaluation of two dimensions. The first dimension considers internal focus and integration versus external focus and differentiation. The second dimension focuses on flexibility and discretion versus stability and control. Choo (2013) applied the Competing Values Framework to an information culture and postulated that an organisation might have one or two dominant information cultures while also valuing other cultures to varying degrees. While this profile was not tested empirically, it provides a visual representation of an information culture, which is valuable both in contextualising the culture and directing change.

The clan culture has, based on a study in Serbia, been found to be one of the cultures that leads to innovation being encouraged in an organisation (Colovic and Williams, 2020). Some of the reasons for this are related to knowledge sharing and communication, both of which are pertinent in the clan culture (Colovic and Williams, 2020), and there is also a link to domain-relevant skills, which are required for creativity. Innovation is applied to identify and solve new information security problems and the solutions are then shared with the group as part of knowledge sharing and communication. A further study in Brazil also found the clan culture, as well as the adhocracy culture, to be conducive to innovation and creativity, whereas the hierarchical type of culture did not have an influence on innovation (Scaliza *et al.*, 2022). The adhocracy culture was also found to have the most impact on innovativeness in universities (Gorzelany, Gorzelany-Dziadkowiec, Luty, Firlej, Gaisch, Dudziak and Schott, 2021). This is supported by the work of Makumbe (2021) in Zimbabwe. Ogbeibu, Senadjki and Luen Peng (2018) also proposed that the clan and adhocracy organisational cultures might positively influence employee creativity but found in a further study in a manufacturing organisation that clan and rational organisational culture have a negative effect on employee creativity, while the hierarchy organisational culture has no effect (Ogbeibu, Senadjki and Gaskin, 2018). The flexibility and external orientation traits of the adhocracy organisational culture favour innovation. Cameron and Quinn (2011) explain that the adhocracy culture supports the generation of new ideas, innovation, and creativity. However, in a study conducted in Brazil in the T-Kibs organisations, it was found that the market culture supports innovation, whereas the clan, adhocracy, and hierarchical organisational cultures did not have an influence on innovation in this study (Bianchi *et al.*, 2021). Further research confirmed that the clan and rational culture have a positive influence on creativity; however, it was also established that the influence of the clan culture on creativity did not appear to be affected by whether computer-mediated communication or face-to-face communication was used, nonetheless, the rational culture was influenced positively (Scheibe and Gupta, 2017). The culture that supports creativity and innovation therefore varies, based on the industry or type of organisation being researched. However, group and adhocracy cultures mostly seem to support creativity and innovation.

A study in Pakistan measured the influence of five constructs, namely, external orientation, organisational climate, flexibility to change, teamwork, and employee empowerment, on innovation performance in an organisation and found that all five constructs positively correlate with innovation performance (Shahzad *et al.*, 2017). They concluded that an organisation should aim to promote research and development activities to contribute to innovation.

Javanmardi Kashan *et al.* (2021) identified 12 innovation values (risk tolerance, creativity, trust, empowerment, flexibility, teamwork and collaboration, employee recognition, diversity, external orientation, learning, continuous development, and proactivity) with 33 underlying cultural dimensions that can positively contribute to an innovation culture. These factors were identified through a literature review and interviews with experts in the mining industry in Australia. While the findings are specific to the mining industry with its unique culture of risk and rigid structures, the findings can still be applicable to relevant contexts to drive innovation as part of the organisational culture (Javanmardi Kashan *et al.*, 2021). The authors also use the organisational cultural levels of Schein to explain that a culture of innovation will be perceived at an abstract, values-and-belief level and that such a culture is “built, promoted, reinforced and communicated through behaviours, practices and artefacts” (Javanmardi Kashan *et al.*, 2021: 3). Employee creativity can be positively influenced when knowledge sharing is taking place and if employees are motivated (Andleeb *et al.*, 2020). A further study, conducted in Romania, found that employees consider autonomy as a positive contributor to being creative (Cuicui *et al.*, 2014) and that innovation supports risk-taking while also enabling trust in organisations (Hwang and Choi, 2017). Table 2 outlines the elements, extracted and summarised from the literature, that can stimulate creativity and innovation as part of the organisational culture.

**Table 2.** Stimulating creativity and innovation elements

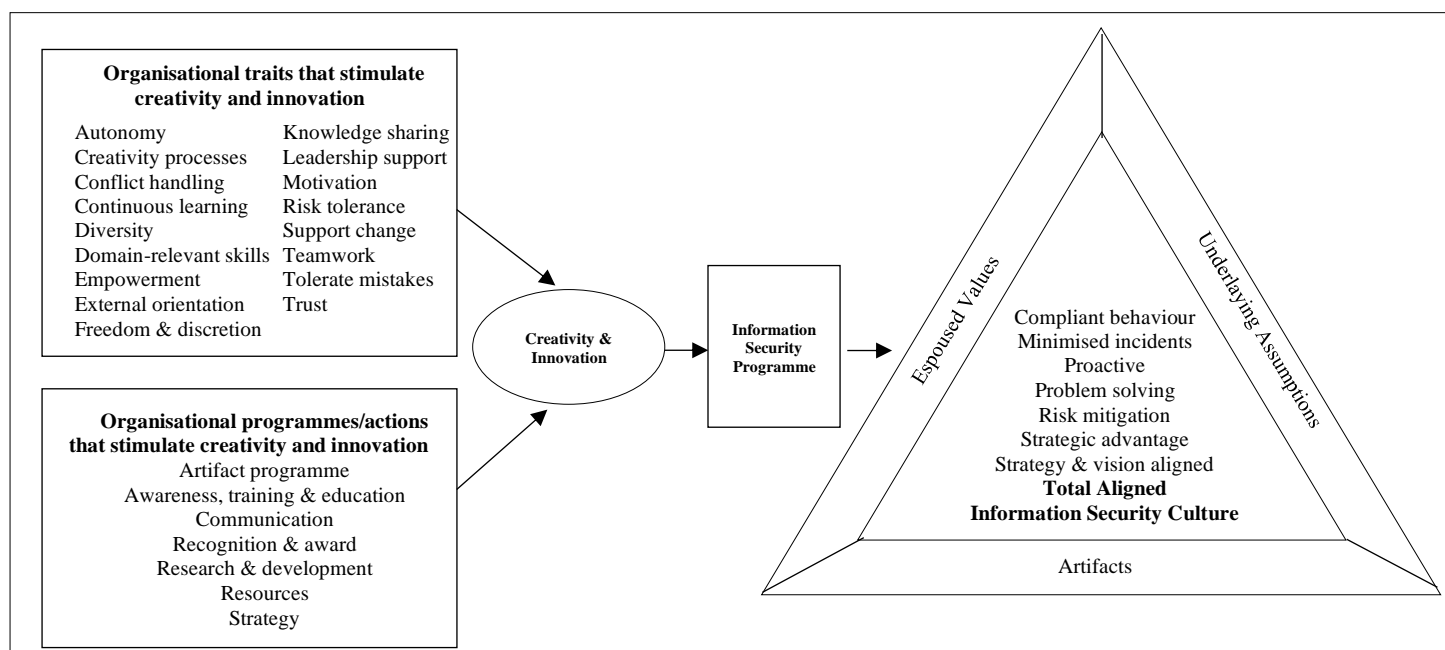
<b>Elements that can stimulate creativity and innovation as part of the organisational culture</b>	
Artifact programme (Hwang and Choi, 2017)	Knowledge sharing (Colovic and Williams, 2020; Javanmardi Kashan <i>et al.</i> , 2021)
Autonomy (Cuicui <i>et al.</i> , 2014; Javanmardi Kashan <i>et al.</i> , 2021; Martins <i>et al.</i> , 2004)	Leaders who challenge, support, and empower staff to generate new ideas (Martins <i>et al.</i> , 2004)
Awareness, training, and education on organisational, group and individual levels (Hwang and Choi, 2017; Lin and Wittmer, 2017)	Research and development activities (Shahzad <i>et al.</i> , 2017)
Continuous learning and development (Javanmardi Kashan <i>et al.</i> , 2021)	Resources (Martins <i>et al.</i> , 2004)

<b>Elements that can stimulate creativity and innovation as part of the organisational culture</b>	
Creativity-relevant processes and behaviour (Martins <i>et al.</i> , 2004)	Risk tolerance (Javanmardi Kashan <i>et al.</i> , 2021; Martins <i>et al.</i> , 2004; Shahzad <i>et al.</i> , 2017)
Communication: formal and informal communication (Colovic and Williams, 2020; Hwang and Choi, 2017); value free, open and transparent (Martins <i>et al.</i> , 2004)	Strategy that supports creativity and innovation (Martins <i>et al.</i> , 2004)
Conflict handling (Martins <i>et al.</i> , 2004)	Supports change, flexible (Javanmardi Kashan <i>et al.</i> , 2021; Martins <i>et al.</i> , 2004; Shahzad <i>et al.</i> , 2017)
Diversity (Javanmardi Kashan <i>et al.</i> , 2021; Martins <i>et al.</i> , 2004)	Task motivation: extrinsic (reward and recognition) (Ambile T.M., 1996; Javanmardi Kashan <i>et al.</i> , 2021; Lin and Wittmer, 2017; Martins <i>et al.</i> , 2004; Padayachee, 2012) and intrinsic motivation (Ambile T.M., 1996; Lin and Wittmer, 2017; Padayachee, 2012)
Domain-relevant skills (Ambile T.M., 1996; Colovic and Williams, 2020)	Teamwork and collaboration (Javanmardi Kashan <i>et al.</i> , 2021; Martins <i>et al.</i> , 2004; Shahzad <i>et al.</i> , 2017)
Employee empowerment (Javanmardi Kashan <i>et al.</i> , 2021; Shahzad <i>et al.</i> , 2017)	Tolerate mistakes (Martins <i>et al.</i> , 2004)
External orientation (Javanmardi Kashan <i>et al.</i> , 2021; Shahzad <i>et al.</i> , 2017)	Trust (Javanmardi Kashan <i>et al.</i> , 2021; Martins <i>et al.</i> , 2004)
Freedom and discretion (Martins <i>et al.</i> , 2004)	

### 3.1.3 Conceptual information security culture model enabled through creativity and innovation

The conceptual information security culture model, enabled through creativity and innovation, is depicted in figure 2. The concepts applied in the model were derived from the literature review summary in table 2, grouped according to either organisational traits or programmes that the organisation can implement to stimulate creativity and innovation as presented in Da Veiga (2022).

**Figure 2.** Information security culture enabled through creativity and innovation (Da Veiga 2022)



The model displays that organisations can implement certain organisational traits to stimulate creativity and innovation. For some organisational cultures, such as the clan or group culture, certain traits – for instance, open communication or teamwork – will already be part of the organisational culture. Creativity and innovation are an output that is applied in the context of information security within the organisation. The information security programme block in the model refers to the people, process, technology, governance, and regulatory aspects of information security within the organisation, encapsulating all aspects of information and cyber security. These could relate to applying creativity to the way information security policies are written, an innovative approach for information security awareness, innovative solutions to aid employees in combating phishing attacks and encouraging employees to apply creative thinking to resolve security issues and problems, as examples.

The model depicts that creativity and innovation stimulate a totally aligned information security culture whereby security is part of the organisation's strategy and vision. Employees display compliant behaviour and adapt their behaviour in creative and innovative manners to combat security threats. Information security is regarded as a strategic advantage resulting in minimised security incidents, especially from a human perspective, as stimulated through creative and innovative problem-solving by employees. Risk mitigation is part of such a culture, with proactive management, problem-solving, and monitoring of information security. The model postulates that, if creativity and innovation can be stimulated in an organisation as part of the organisational culture and specifically translated to the information security culture, it will assist in establishing a strong and totally aligned security culture, on a values, assumptions, and artifact level – one where the risk of the human element is minimised and converted to become a contributing element in combatting security risks and threats through creativity and innovation.

## **3.2 Phase 2: Expert panel review**

Phase 2 of the research method comprised of the expert panel review to validate and refine the proposed conceptual model that was presented in figure 2.

### **3.2.1 Method**

The expert panel participants were selected using the purposive sampling technique to identify specific individuals with the necessary experience based on the judgement of the researcher (Saunders 2016). The expert panel comprised of 11 individuals, three from academia, six from industry and two expert panel participants working in an academic and industry context. Ten of the expert panel participants have a PhD in either industrial psychology or information communication technology. The expert panel participants were from Australia, China, South Africa, and Spain. The experience of the expert panel participants covered both information security and organisational behaviour as well as a technical perspective: seven of the expert panel participants have experience in socio-technical aspects of information (cyber) security, information security behaviour, and information security culture; two expert panel participants have experience in organisational psychology with creativity and innovation; and two expert panel participants have experience in information communication and technology.

Research ethical clearance was obtained from the university's research ethics committee (research ethics certificate number: 2022/CSET/SOC/019) and the principles of voluntary participation, anonymity, confidentiality, and privacy were applied. The identified sample was invited via e-mail to participate and each received an information pack comprising the participant information document, consent form and information about the conceptual model. Each participant signed the consent form. The interviews were conducted during September and October 2022 and lasted up to an hour and a half. All the interviews were conducted online using MS Teams. During the interviews the conceptual model was presented to the expert panel participants whereafter the interview questions were discussed. The interview questions covered the relevance, completeness, applicability, and understandability of the conceptual model (figure 2) as well as the importance and grouping of the elements. The 10 interview questions are included in Appendix A.



The interview discussions were transcribed using the MS Office transcription tool and were downloaded for analysis and interpretation. The researcher applied Cresswell's (2014) qualitative data analysis steps. The data was organised by means of downloading the transcribed files from each MS Team meeting and anonymising the participant information in each file. The files were imported to Atlas.ti and validated for accuracy by reading through it and comparing it to the notes taken during each interview.

Thematic analysis was applied whereby themes were identified throughout the dataset and coding was applied to the units of data (Saunders 2016). The frequency of the concepts and phrases were identified as part of the process to synthesise the data. The main themes were defined based on the interview questions. Further subthemes were identified, and data was coded as represented in the narrative text. The final themes and subthemes were defined following a repetitive analysis process of the transcriptions. The subthemes reached data saturation with the interviews with the 11 expert panel participants and as such the interviews were concluded as new themes were not identified (Cresswell 2014). The final step was the interpretation of the data analysis, and several recommendations were deducted to refine the conceptual model. The results are discussed in section 3.2.2 and were applied to develop the refined model, (ISC-C&I), presented in section 4, figure 4.









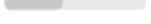
The following were considered to address validity and reliability of the study:

- a) **Credibility:** Ensuring that the data obtained from the expert panel participants are accurate and a true interpretation of their views (Cresswell 2014, Saunders 2016). In this study, the answers of the expert panel participants were confirmed with them during the discussion and notes were compared to the transcribed text.
- b) **Dependability:** Dependability relates to how reliable the study is and if the same findings will be derived in a similar circumstance (Saunders 2016). This relies to an extent on the researcher and the researcher's experience in collecting and interpreting data. The researcher and expert panel participants in this study have experience in information security culture and a structured interview protocol was applied as recommended by Cresswell (2014). The information about the conceptual model publication, interview questions, participant information sheet and consent forms for research ethical clearance were provided to all the expert panel participants.
- c) **Conformability:** This aspect relates to the way the researcher's personal interest results in bias. The researcher is required to be neutral and use a structured approach that can provide an audit trail for deriving the conclusions. This was considered by applying transparency with the expert panel participants and reporting of the process followed and establishing consistency in the coding (Given 2008). The coding and themes were reviewed, checked, and re-checked.
- d) **Transferability:** Transferability applies to the generalisability of the study. A qualitative study's transferability can be improved by documenting the methodological approach with the processes that applied in the study (Saunders 2016). To contribute to transferability the researcher defined selection criteria which were applied and the approach was documented as part of the research methodology.
- e) **Authenticity:** The views and voices of all expert panel participants should be recorded and included to represent the expert panel participants (Given 2008, Saunders 2016). All data of the interview sessions was included in the data analysis and reporting.

### 3.2.2 Results

Figure 3 portrays the qualitative data analysis with nine main themes as coded in Atlas.ti with seven of the themes comprising of subthemes. Most of the comments related to the theme "Extend" where expert panel participants recommended elements that can be added to the conceptual model to extend and improve it further. This was followed by the theme "Encourage" detailing aspects which the expert panel participants believe organisations can do that will encourage or create an environment for employees to enhance creativity and innovation and to create a totally aligned information security culture. The themes and subtheme results are discussed in the sections that follow.

**Figure 3:** Themes in Atlas.ti

Name	Grounded
○ ◆ Comprehensive/Complete (Q4)	 8
○ ◆ Creativity and innovation aiding to combat cyber attacks (Q1)	 9
▷ ○ ◆ Encourage (Q2)	 31
▷ ○ ◆ Extend (Q4)	 39
▷ ○ ◆ Generalisation (Q8)	 24
▷ ○ ◆ Important (Q6)	 18
▷ ○ ◆ Relevant (Q3 & Q5)	 18
▷ ○ ◆ Simplistic (Q9)	 5
▷ ○ ◆ Structure (Q7)	 16

### 3.2.3 Comprehensive

The overall view was that the conceptual model is comprehensive and that the content is supported with the inclusion of the elements derived from the scoping literature review of phase 1. While the expert panel participants felt that the traits included in the conceptual model would make a difference in supporting creativity and innovation in an organisation, they also recommended several elements to extend the model further.

### 3.2.4 Creativity and innovation aiding in combatting cyberattacks

Creativity and innovation could “*have a positive influence*” to combat cyberattacks according to various expert panel participants. This should, however, be managed carefully to not introduce additional risk to the organisation as emphasised by participant C, “*like resilience and adaptability all these types of concepts have a good impact in the performance indicators of the organisations but in other cases in other organisations, they add more risks and they generate more risks if creativity and innovation is not well managed, it can be more risky than encouraging safety or security.*”

Participant G explained that in his/her view creativity and innovation should be encouraged in the way information security awareness is conducted and not necessarily encouraging creativity and innovation in how employees respond to incidents and breaches, “*I don't see this as creativity in response to an attack or threat. It's more about the creativity and innovation in raising awareness and educating people in the development of a culture where there's communication and creative thought on, you know, security, whatever means that is. But from a proactive sense, not in the response, because there will be defined ways that people shouldn't respond...to give them (employees) freedom on how to respond to a cyberattack is, to me, it will be just too risky*”. The context and scope in which creativity and innovation is encouraged in an organisation should therefore be clearly defined.

### 3.2.5 Encourage

The subthemes in table 3 emerged as elements that could encourage or motivate an environment where creativity and innovation are encouraged.

**Table 3:** Encourage subthemes

Encourage subthemes	Count
Encourage: Autonomy	2
Encourage: Buy-in	1
Encourage: Communication	5
Encourage: Discretion	1
Encourage: Freedom	4

<b>Encourage subthemes</b>	<b>Count</b>
Encourage: Identify risks	1
Encourage: Network between teams	1
Encourage: Policies	3
Encourage: Proactiveness	4
Encourage: Problem-solving	1
Encourage: Resilient (prepared to fail)	2
Encourage: Respect	1
Encourage: SETA	4
Encourage: Teamwork within teams	1
<b>Encourage total</b>	<b>31</b>

Participant A mentioned that **autonomy, freedom, and discretion** will encourage an environment where, “*people will identify risks and then have the freedom to come up with creative and innovative problem-solving*” hereby aiding in “*proactively combatting cyberattacks, incidents and other issues*” as postulated by participant B and supported by participant E “*to avoid future problems*”. Participant G, extended creativity and innovation specifically to the manner in which information security **knowledge is conveyed**, “*...convey the knowledge in a creative way and in a better way that things could be addressed, proactively versus not in the reactive sense but in the proactive sense in being creative and innovative in developing that culture*”.

However, creativity and innovation must be carefully managed through the introduction of a **formal decision-making process** or **forum** where ideas can be presented and approved by the **leadership** team as recommended by participant A. Employees should have the freedom to express their ideas, but in a safe environment where the management and staff are “*respectful to people and respecting their opinions*” (participant J).

Expressing ideas in a safe forum and approving/rejecting ideas through a formal decision-making process must be conducted within the boundaries of **policies** in the organisation. Policies play a critical role in either encouraging or discouraging creativity and innovation. In some instances, policies are rigid and one “*cannot use it in complex and uncertain environments. So, in these situations, creativity will be very important because people cannot predict the future situation and they need to respond to these kind of disasters or emergencies at the first right time and employees sometimes need to apply their own choices, their own decision making*”, according to participant F. However, employees cannot have free reign as it could introduce risk and compliance with policies are still expected. The policies can though be tailored to support creativity and innovation within certain boundaries as explained by participant G, “*there's red tape, there's policies that have got to be followed and of course the policies have a place, but perhaps organisations need to look at those policies to see how they could support creativity and innovation...the policy comes in where management in the policy needs to create the limit of the creativity to an extent...that policy, I think, is what's going to determine the boundaries of creativity and innovation.*”

While a forum to present ideas could encourage creativity and innovation, it will also be important to create a **resilient culture** where employees are allowed to present ideas even though it might fail according to participant I, “*For me, something that stands out is focusing on having a resilient workplace, because if you want people to be innovative and creative, they also have to be prepared to fail and I think that's difficult for some organisational settings.*” This was supported by participant K, who emphasised the important role of **management support and attitude** to tolerate failure, “*If you're going to encourage creativity and innovation, the chance of failure is going to go up. So, if they're going to focus on one thing, it should be focusing on maybe management attitude.*”

“*Communication and information are crucial*” to facilitate creativity and innovation according to participant C. Participant G explained it further by referring to **two-way communication**, “*Creativity and innovation create an*

environment where people do talk. It's not top down, it's probably more bottom up I suppose or two-way, two-way communication. So, it's not top down, it's getting collaboration going or getting discussions going about it." **Team-work** was also emphasised as an important aspect to encourage creativity and innovation "where one would not only focus on encouraging creativity within the teams, but also the networking between different teams so that they support each other, know what the other teams are doing and what type of risks and problems there are that need to be solved..." (participant A).

### 3.2.6 Extend

The majority of the discussions related to recommendations to extend the conceptual model as indicated in table 4 with the related frequencies of each subtheme.

**Table 4:** Extend subthemes

<b>Extend subthemes</b>	<b>Count</b>
Extend: Aims and goals that focus on innovation and creativity	1
Extend: Balance (work vs security; risk; negative/positive impact)	5
Extend: Communication tools	1
Extend: Decision-making process, guidelines, boundaries	3
Extend: External factors	3
Extend: Induction & onboarding	1
Extend: IS programme	3
Extend: IT expert	2
Extend: Management final decision	2
Extend: Organisational cultures (4 types)	1
Extend: Performance measurement	1
Extend: Policy	2
Extend: Recruitment of specific profile/right people	2
Extend: Risk appetite/level	4
Extend: Roles and responsibilities	1
Extend: Security expert	1
Extend: Subcultures (departments, job levels, etc)	3
Extend: Technical	3
<b>Extend total</b>	<b>39</b>

A balance between work efficiency versus security controls and the negative versus positive impact of creativity in information security needs to be achieved (participant C). This relates to the discussion around the **risk profile (appetite)** of an organisation whereby certain industries such as financial or military organisations will be highly regulated and limited creativity and innovation will be tolerated (participant G). Participant D also supported the consideration of the risk appetite and stated that, "the purpose of each organisation is different. Perhaps the level of risk should be restricted if they have nuclear weapons or something like that, for example, perhaps they have to follow strict protocols of security." The management of creativity and innovation becomes critical to ensure that the risk appetite is considered, "So it's the risk assumption, the amount of risk that the organisation will manage... they have to manage it correctly", participant C. Expert panel participants commented about the risk appetite the most and suggested that the model be extended to incorporate the concept of considering the risk appetite of an organisation and potential risk that could be introduced when encouraging creativity and innovation. This can further be managed through **policy** as participant G recommended, "The policy comes in where management in the policy needs to create the limit of the creativity to an extent" as well as management approval (participants A and J). Furthermore, the **roles and responsibilities** for the enhancement of creativity and innovation must also be defined, "roles and responsibilities of each department of the organisation or of each person in the organisation", participant C.

In terms of incorporating a **decision-making process**, participant A stated that, “...*innovative ideas that need to be implemented need to be proposed to the leadership team and then approved by them...deciding whether it's a feasible thing to implement or whether it should be changing certain ways or totally discarded, and so I think in terms of the decision-making, there needs to be a process in place that would encourage people to bring forward their creative ideas and problem-solving and then the process needs to be done properly so that people are not discouraged by saying oh, this idea is definitely not a good one – it won't work*”.

The **IS programme** block in the conceptual model can be unpacked further to understand what the IS programme would entail (participant F, I and K), as recommended by participant I, “*put some more points in that square like training programmes, different things that the organisation actually does.*”

If an organisation aims to enhance creativity and innovation, they need to pay attention to the **recruitment** of the correct people, “*people who are inclined to be creative and innovative in the first place*”, according to participant A. It was also mentioned that creativity and innovation should be restricted to **IT experts** or **security experts** and not all employees in the organisation as it could introduce risk (participant D). The employees who will be expected or encouraged to exhibit creativity and innovation should therefore be defined and recruited accordingly.

There was also a recommendation to extend the model to be considerate of **subcultures**, which could, for example, “*it can be subcultures related with the hierarchy or with the seniority or with the type of contract maybe*”, - participant C; “*subcultures in the different departments*” - participant G; “*different parts of the organisation will present in very different ways in terms of how their culture looks and how people behave and interact*” - participant I.

**External factors** should be incorporated in the model, namely, social factors (participant C); national strategy such as strategies from government or regulatory bodies (participant E) and other external factors such as market challenges or even cyber incidents (participant J). Participants C and E also recommended adding a **technical** element to the model as the technology could also influence the creativity and innovation whereas technology used in a university or research body will be different.

Other specific aspects which expert panel participants recommended to be added were:

- **Communication tools:** “*I would include communication tools – a fast communication tool between the employees and the IT team for example*”, participant D.
- **Performance measurement:** Participant B recommended adding performance measurement to the model, “*Because I think many times organisations measure all the other aspects, but not things connected to the norms and the values which is linked to what you're trying to measure.*”
- **Onboarding:** Participant B further recommended adding onboarding that incorporates information security aspects, “*It's very specifically focused and what's interesting about it, is that it focuses on aspects like policies and procedures, roles and expectations and then links very nicely to information security also focusing on organisational norms and values.*”
- **Organisational culture:** Participant B also recommended considering an inclusion of the four organisational cultures in the model, namely, the Hierarchy, Market (Rational), Clan (Group) and Adhocracy (Developmental) cultures.

### 3.2.7 Generalisation

The expert panel felt that the conceptual model is applicable, however the application of the model could vary based on a number of factors such as sectors (financial, health, government, etc.), departments within an organisation, subcultures within an organisation, organisations with different organisational cultures and organisations in different countries (see table 5). A critical aspect to consider for generalisation will be the risk profile of the organisation and to what extent creativity and innovation could contribute to create a strong information security culture versus introducing risk.

**Table 5:** Generalisation subthemes

Generalisation subthemes	Count
Generalisation: Applicable	6
Generalisation: Different between countries	2
Generalisation: Different across organisational culture	2
Generalisation: Different across departments	3
Generalisation: Different across sectors	6
Generalisation: Different risk profile	5
<b>Generalisation total</b>	<b>24</b>

### 3.2.8 Important

The expert panel was asked to recommend traits or elements which they believe are most important to enhance creativity and innovation in an organisation. The recommendations are listed in table 6. Two traits were mentioned a few times by the various expert panel participants, namely, **freedom** and **discretion**, “*to have the freedom and discretion to be creative and they have that autonomy to go to go ahead, which would speed up things*” – participant A; and **trust** was also an important concept, “*trust which you know the to be able to know that, you know, trusting the processes or trusting the systems perhaps ties all the others together*” – participant G. A third concept that was emphasised by participant K was **leadership** “*ensuring that the leadership understands how to develop innovation*” which was supported by participant C, “*If creativity and innovation is not pushed from the upper levels, it won't take place.*”

**Table 6:** Importance subthemes

Important subthemes	Count
Important: Autonomy	2
Important: Diversity	1
Important: Freedom and discretion	3
Important: Governance	1
Important: Individual motivation	1
Important: Information security programme	1
Important: Leadership	3
Important: Respect	2
Important: Teamwork	2
Important: Trust	2
<b>Important total</b>	<b>18</b>

### 3.2.9 Relevance

The expert panel participants indicated that the model as a whole, as well as the individual elements are relevant (table 7). Participant A recommended that all elements in the model should be defined within organisations to establish the context of each element and how to apply or adapt it in each working environment. Participant I felt that the model will be more suited for larger organisations, “*this model would be most suited to larger organisations, because I you need the structure that larger organisations present. So large organisations have a lot of resources, they have strategies and policies in place, they have funding available for research and development. So, I think potentially you can get the most value out of this when you are focusing on those larger, more corporate sort of settings.*”

**Table 7:** Relevance subthemes

<b>Relevant subthemes</b>	<b>Count</b>
Relevant: All elements	7
Relevant: Define elements	1
Relevant: Large organisations (policies, resources, strategies)	1
Relevant: Model (Yes)	7
Relevant: Some traits harder to change	1
Relevant: Time frame to monitor change	1
<b>Relevant total</b>	<b>18</b>

Participant K was interested in the time frame necessary to see a change in the creativity and innovation in an organisation, *“Some of those things in that second box there, the programmes and actions that you can take as an organisation, you know, how long would you expect that to flow into some measurable change in the security state of things? It’ll be interesting to see how long that takes.”* Participant J pointed out that some of the traits might be harder to change in an organisation, *“The only thing would be that the organisational traits that stimulate creativity, innovation, some of them may be much harder to change.”*

### 3.2.10 Simplistic

The expert panel participants felt that the conceptual model is simplistic enough to understand as emphasised by five of the respondents, but that it could be simplified when statistical analysis such as structural equation modelling is done in future. One participant (participant F) felt that there might be too many traits and that some of these traits could be combined for an even more simplistic model.

### 3.2.11 Structure

The expert panel participants were comfortable with the grouping of the elements in either the trait or programme blocks of the conceptual model; see table 8. However, to further refine the model they recommended to incorporate levels in which more strategic and managerial aspects, for example, can be grouped in a level. Participant C explained that *“I think that all these factors are traits, but I think that some of them are not on the same level, some of them depend on the others”* and aspects on an *“individuals level or organisational level such as the strategy”*, can be grouped together as recommended by participant F. This can be further explored with statistical analysis, such as structural equation modelling to further group the elements as recommended by participants B and C. Participant G also mentioned that it might be interesting to group the elements according to the three areas which Robbins et al. (2018) discuss that can be focused on to achieve creativity and innovation, namely, *“expertise, creative thinking skills and intrinsic task motivation”*.

**Table 8:** Structure subthemes

<b>Structure subthemes</b>	<b>Count</b>
Structure: Grouping to improve	3
Structure: Grouping is good	5
Structure: Levels to be added	5
Structure: Refine with SEM	3
<b>Structure total</b>	<b>16</b>

#### **4 Validated and refined information security culture model with creativity and innovation as enablers (ISC-C&I Model)**

The conceptual model in figure 2 was refined to incorporate the recommendations of the expert panel review. Figure 4 portrays the refined and validated information security culture model with creativity and innovation as enablers (ISC-C&I Model).

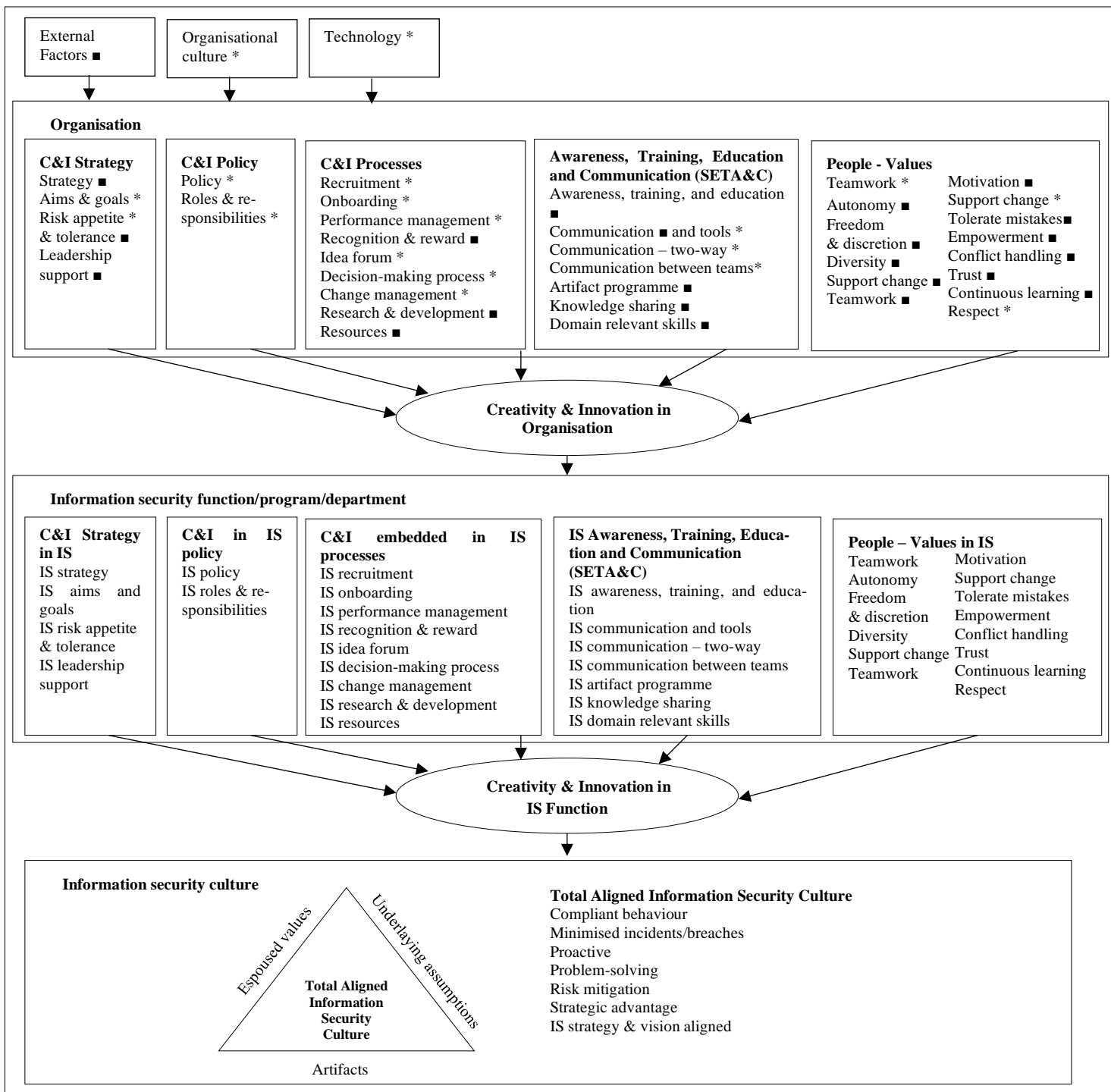
Creativity and innovation can purposefully be encouraged in an organisation through various elements which are grouped in the following categories (or levels): creativity and innovation (C&I) strategy, C&I policy, a C&I process; awareness training, education, and communication (SETA&C) and people values. These elements were extracted from the literature review (■) and enhanced with 18 elements deducted from the expert panel review (\*) and are encouraged on an organisational level to establish an overall culture of creativity and innovation. Each organisation will though have an embedded organisational culture (e.g., the Clan culture), which might encourage or another culture (e.g., Hierarchy culture), which does not encourage creativity and innovation. The existing organisational culture needs to be considered as an external factor which could influence the decision to promote and encourage creativity and innovation in an organisation as well as the success thereof. External factors can also play a role as to whether an organisation will purposefully encourage creativity and innovation such as the economy, competition, regulatory requirements, and industry requirements. For example, if there are prescriptive requirements from government or an industry standard it could minimise the freedom to develop innovative solutions and approaches. The intention is to embed a culture of creativity and innovation within the organisational culture which then serves as a platform to further embed a culture of creativity and innovation in the information security function.

The elements in the categories on the organisational level are replicated in the information security function (programme and/or department): creativity and innovation (C&I) strategy in information security (IS), C&I in IS policy, C&I in IS processes; IS awareness training, education, and communication (SETA&C), and people values in IS. Creativity and innovation are encouraged in the information security function, starting by incorporating creativity and innovation in information security strategy and defining the boundaries thereof in policies and roles and responsibilities while considering the risk appetite and tolerance of the organisation. Various processes can be embedded to further stimulate creativity and innovation, such as onboarding where information security is incorporated together with the values that are encouraged. New ideas and solutions can be presented in the information security ideas forum and approved through the decision-making process in the information security department. Employees must continue to comply with information security policies and follow defined information security processes to use information and communication technology, to process data, and to report and deal with information security breaches and incidents. Employees should, however, not apply creativity and innovation outside of formal information security policies and processes. Employees are encouraged though to submit and present ideas at the creativity and idea forum on an organisational level as well as within the information security department together with information security experts. Approved ideas can further be researched and developed utilising provided resources and implementing it through change management programmes. Creativity and innovation are specifically embedded in the communication and awareness of information security requirements to staff, encouraging cross-team communication and aiming to equip employees in the information security function and wider organisation with information security skills. Performance management and recognition and reward processes can be used to motivate creativity and innovation within the security function. The values in figure 4 should be strived for and incorporated as part of the information security strategy, policies, and processes to further encourage creativity and innovation.

The aim is to encourage creativity and innovation within the information security function to establish a totally aligned information security culture (triangle in figure 4) that relates to minimised incidents and breaches, proactiveness, problem-solving, and risk mitigation to contribute to becoming cyber resilient. Over time this will then become part of the information security culture which will be evidenced in the artifacts, values, and behaviour exhibited in the information security function and wider organisation.



**Figure 4:** Information security culture model with creativity and innovation as enablers (ISC-C&I Model)



## 5 Contribution to practice and research

It is envisaged that the information security culture model with creativity and innovation as enablers (ISC-C&I Model) can be applied in organisations to stimulate creativity and innovation as traits of an information security culture and with the aim of mitigating security risks and threats from a human perspective. The model will serve as a point of reference for further academic work to investigate the influence of creativity and innovation on the information security culture.

## 6 Limitations

The information security culture model with creativity and innovation as enablers (ISC-C&I Model) was developed using a qualitative approach and the relationships and influences of the various elements have not been established. It is recommended that future studies expand the model to validate it further by using structural equation modelling. It is also acknowledged that the impact of creativity and innovation on the information security culture is postulated and that it must be evaluated in different organisations and industries using an extended empirical approach.

## 7 Conclusion

An investigation was conducted into what an information security culture model would comprise where innovation and creativity are used as enablers. The study provided a foundation to propose a conceptual model whereby information security culture is enabled through creativity and innovation. Key traits to stimulate creativity and innovation in an organisation were identified, such as support for change, diversity, autonomy, teamwork, and trust. Certain organisational programmes also enable creativity and innovation, such as an artifact programme, education, training and awareness, communication and recognition, and rewards. The model was refined and validated with an expert panel review who recommended 18 additional elements to extend the model. Implementing creativity and innovation in an information security context within an organisation must be done in cognisance of the organisational risk profile and tolerance whilst being managed carefully through a strategy and related policies that define the boundaries of creativity and innovation. Value can be added by incorporating creativity and innovation in information security education, awareness, training, and communication to enable knowledge sharing and establish information security domain relevant skills amongst employees. A limitation of the paper is that the model has not been validated statistically. Future research will need to employ a quantitative research method to validate the model using structural equation modelling.

## References

- AlHogail, A. (2015), "Design and validation of information security culture framework", *Computers in Human Behavior*, Vol. 49, pp. 567–575.
- Ambile T.M. (1996), *Creativity in Context*, Westview Press, Boulder, CO.
- Andleeb, N., Ahmad, M.F., Hassan, M.F., Rahman, N.A.A., Abdullah, A.S. and Nawi, M.N.M. (2020), "Linkage of Knowledge Sharing, Organizational Culture, Supply Chain Strategies towards Employee Creativity in Manufacturing Organizations", *International Journal of Supply Chain Management*, Vol. 9 No. 4, pp. 132–140.
- Auernhammer, J. and Hall, H. (2014), "Organizational culture in knowledge creation, creativity and innovation: Towards the Freiraum model", *Journal of Information Science*, Vol. 40 No. 2, pp. 154–166.
- Bianchi, C.E., Tontini, G. and Gomes, G. (2021), "Relationship between subjective well-being, perceived organisational culture and individual propensity to innovation", *European Journal of Innovation Management*, Emerald Group Holdings Ltd., Vol. ahead-of-print No. ahead-of-print, pp. 1460–1060.
- Cameron, K.S. and Quinn, R.E. (2011), *Diagnosing and Changing Organizational Culture: Based on the Competing Values Framework*, Jossey-Bass, San Francisco, CA.
- Choo, C.W. (2013), "Information culture and organizational effectiveness", *International Journal of Information Management*, Vol. 33 No. 5, pp. 775–779.
- Colovic, A. and Williams, C. (2020), "Group culture, gender diversity and organizational innovativeness: Evidence from Serbia", *Journal of Business Research*, Vol. 110, pp. 282–291.
- Cresswell. J.W. (2014), "Research design" Sage: Los Angeles.

- Cuicui, R.A., Mateescu, V. and Cuicui, I. (2014), “Organizational Culture and Innovation: An Industrial Case Study”, in Meersman, R., Panetto, H., Mishra, A., Valencia-García, R., Soares, A.L., Ciuciu, I., Ferri, F., et al. (Eds.), *On the Move to Meaningful Internet Systems: OTM 2014 Workshops, Lecture Notes in Computer Science*, Vol. 8842, Springer-Verlag, Berlin, pp. 514–518.
- Da Veiga, A. (2019), “Achieving a Security Culture”, *Cybersecurity Education for Awareness and Compliance*, pp. 72–100.
- Da Veiga, A. (2021), “Information Security Culture”, *Encyclopedia of Cryptography, Security and Privacy*, Springer Berlin Heidelberg, pp. 1–4.
- Da Veiga, A. (2022). “A Model for Information Security Culture with Innovation and Creativity as Enablers”. In: Clarke, N., Furnell, S. (eds) *Human Aspects of Information Security and Assurance. HAISA 2022. IFIP Advances in Information and Communication Technology*, vol 658. Springer, Cham.
- Da Veiga, A., Astakhova, L.V., Botha, A. and Herselman, M. (2020), “Defining organisational information security culture—Perspectives from academia and industry”, *Computers and Security*, Vol. 92, available at: <https://doi.org/10.1016/j.cose.2020.101713>.
- ENISA. (2017), *Cyber Security Culture in Organisations*, European Union Agency for Network and Information Security (ENISA), available at: <https://doi.org/10.2824/10543>.
- Gorzelany, J., Gorzelany-Dziadkowiec, M., Luty, L., Firliej, K., Gaisch, M., Dudziak, O. and Schott, C. (2021), “Finding links between organisation’s culture and innovation. The impact of organisational culture on university innovativeness”, *Plos ONE*, Vol. 16 No. 10.
- Grant, M.J., Booth, A. and Centre, S. (2009), “A typology of reviews: An analysis of 14 review types and associated methodologies”, *Health Information & Libraries Journal*, Vol. 26 No. 2, pp. 91–108.
- Given L.M. (2008), “The Sage encyclopedia of qualitative research methods”, Vol 1& 2, Sage: Los Angeles.
- Gregor, S. and Hevner, A. (2013). “Positioning and Presenting Design Science Research for Maximum Impact”, *MIS Quarterly*. Vol. 37, pp. 337-356. 10.25300/MISQ/2013/37.2.01.
- Hayden, L. (2016), *People-Centric Security. Transforming Your Enterprise Security Culture*, McGraw-Hill Education, New York.
- Hwang, K. and Choi, M. (2017), “Effects of innovation-supportive culture and organizational citizenship behavior on e-government information system security stemming from mimetic isomorphism”, *Government Information Quarterly*, Vol. 34 No. 2, pp. 183–198.
- Javanmardi Kashan, A., Wiewiora, A. and Mohannak, K. (2021), “Unpacking organisational culture for innovation in Australian mining industry”, *Resources Policy*, Vol. 73 No. 2021, p. 1021249.
- Lin, C. and Wittmer, J.L.S. (2017), “Proactive Information Security Behavior and Individual Creativity: Effects of Group Culture and Decentralized IT Governance”, *IEEE International Conference on Intelligence and Security Informatics: Security and Big Data*, IEEE International Conference on Intelligence and Security Informatics: Security and Big Data, pp. 1–6.
- Makumbe, W. (2021), “The impact of organizational culture on employee creativity amongst Zimbabwean academics”, *African Journal of Science, Technology, Innovation and Development*, Taylor and Francis Ltd., available at: <https://doi.org/10.1080/20421338.2020.1864882>.
- Martins, E., Martins, N. and Terblanche, F. (2004), “An organisational culture model to stimulate creativity and innovation in a university library”, *Advances in Library Administration and Organization*, JAI Press, Vol. 21, pp. 83–130.
- Martins, E.C. and Meyer, H.W.J. (2012), “Organizational and behavioral factors that influence knowledge retention”, *Journal of Knowledge Management*, Vol. 16 No. 1, pp. 77–96.
- Martins, E.C. and Terblanche, F. (2003), “Building organisational culture that stimulates creativity and innovation”, *European Journal of Innovation Management*, Vol. 6 No. 1, pp. 64–74.
- Mimecast. (2022), *Confronting the New Wave of Cyberattacks – The State of Email Security 2022*, available at: <https://www.mimecast.com/globalassets/documents/ebook/state-of-email-security-2022.pdf> (accessed 10 March 2022).
- Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G. and Group, P. (2009). *Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement*, available at: [www.annals.org](http://www.annals.org).
- Niekerk, J. and Von Solms, R. (2005), “A holistic framework for the fostering of an information security sub-culture in organizations”, *Issa*, pp. 1–13.
- Oates, B.J. (2012), *Researching information systems and computing*, Sage: Los Angeles.

- Ogbeibu, S., Senadjki, A. and Gaskin, J. (2018), "The moderating effect of benevolence on the impact of organisational culture on employee creativity", *Journal of Business Research*, Vol. 90, pp. 334–346.
- Ogbeibu, S., Senadjki, A. and Luen Peng, T. (2018), "An organisational culture and trustworthiness multidimensional model to engender employee creativity", *American Journal of Business*, Emerald, Vol. 33 No. 4, pp. 179–202.
- Padayachee, K. (2012), "Taxonomy of compliant information security behavior", *Computers and Security*, Vol. 31 No. 5, pp. 673–680.
- Quinn, R.E. and Rohrbaugh, J. (1983), "A spatial model of effectiveness criteria – Towards a competing values approach to organizational analysis", *Management Science*, Vol. 29 No. 3, pp. 363–377.
- Robbins, S.P., Judge, T.A., Odendaal, A. and Roodt, G. (2018), *Organisational Behaviour – Global and Southern African Perspectives*.
- Saunders, M., Lewis, P., and Thornhill, A. (2016), "Research methods for business students", seventh edition, Pearson: Harlow, England.
- Scaliza, J.A.A., Jugend, D., Chiappetta Jabbour, C.J., Latan, H., Armellini, F., Twigg, D. and Andrade, D.F. (2022), "Relationships among organizational culture, open innovation, innovative ecosystems, and performance of firms: Evidence from an emerging economy context", *Journal of Business Research*, Vol. 140, pp. 264–279.
- Scheibe, K.P. and Gupta, M. (2017), "The effect of socializing via computer-mediated communication on the relationship between organizational culture and organizational creativity", *Communications of the Association for Information Systems*, Association for Information Systems, Vol. 40 No. 1, pp. 294–314.
- Schein, E.H. (1985), *Organizational Culture and Leadership*, Jossey-Bass, San Francisco.
- Schlienger, T. and Teufel, S. (2002), "Information Security Culture: The Socio-Cultural Dimension in Information Security Management", *Proceedings of the IFIP TC11 17th International Conference on Information Security: Visions and Perspectives*, pp. 191–202.
- Shahzad, F., Xiu, G.Y. and Shahbaz, M. (2017), "Organizational culture and innovation performance in Pakistan's software industry", *Technology in Society*, Vol. 51, pp. 66–73.
- Von Solms, R. and Van Niekerk, J. (2013), "From information security to cyber security", *Computers & Security*, Vol. 38, pp. 97–102.
- Smith, R. (2019). "A co-creation design framework to support elderly rural women in refining an ICT platform" Doctoral thesis, University of Pretoria, South Africa, <https://repository.up.ac.za/handle/2263/71768>.
- Strychalska-Rudzewicz, A. and Rudzewicz, A. (2021), "The impact of organizational innovativeness on firm performance in Poland. The moderating role of innovation culture", *European Research Studies Journal*, Vol. XXIV No. 3, pp. 130–148.
- Tolah, A., Furnell, S.M. and Papadaki, M. (2021), "An empirical analysis of the information security culture key factors framework", *Computers and Security*, Vol. 108, available at: <https://doi.org/10.1016/j.cose.2021.102354>.

**Appendix A: Interview questions**

<b>Questions</b>
1. In your opinion, do you think creativity and innovation can aid to encourage employees to combat cyberattacks and incidents?
2. In your opinion, what do you think can organisations do that will motivate/encourage/create an environment for employees to use creativity and innovation to combat or solve cyberattacks and incidents?
3. How relevant is the model for organisations? (Focusing on the relevance as part of validity and efficiency, (Gregor & Hevner 2013; Smith 2019)).
4. Is the model complete? What is missing (omitted) in the model? (Focusing on completeness as part of utility, (Gregor & Hevner 2013; Smith 2019))
5. How relevant are the components in the model? (Which features are irrelevant? / Which features are relevant?) (Focusing on the relevance as part of the validity, (Hevner 2013; Smith 2019)).
6. Which of the elements in the model do you think are most important to stimulate creativity and innovation? (Focusing on importance as part of efficiency, (Hevner 2013, Smith 2019)).
7. Do you agree with the grouping of the elements in the categories? (Focusing on grouping and categories as part of quality and simplicity, (Gregor & Hevner 2013; Smith 2019)).
8. Would the model be applicable in different environments? (Generalization) (Consideration of generalization due to qualitative nature of study, (Creswell 2014)).
9. Is the model simplistic enough (clear) to understand? (Focusing on simplicity in terms of quality, (Gregor & Hevner 2013; Smith 2019))
10. Other question/s or discussion/s that might arise based on the questions above.