PREPRINT

UNEDITED VERSION PUBLISHED IN

Information & Computer Security, Vol. 12, Issue 5, 2018

To cite this document:
Adéle Da Veiga, (2018) "An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture", Information & Computer Security, Vol. 26 Issue: 5, pp.584-612, https://doi.org/10.1108/ICS-08-2017-0056
Permanent link to this document:
https://doi.org/10.1108/ICS-08-2017-0056

An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture

Adéle da Veiga

College of Science, Engineering and Technology, School of Computing, University of South Africa, P.O. Box 392, UNISA 0003, South Africa

dveiga@unisa.ac.za

Abstract

Purpose: Employee behaviour is a continuous concern owing to the number of information security incidents resulting from employee behaviour. The aim of this research is to propose an approach to information security culture change management that integrates existing change management approaches, such as the ADKAR model of Prosci, and the Information Security Culture Assessment (ISCA) diagnostic instrument (questionnaire), to aid in addressing the risk of employee behaviour that could compromise information security.

Design/methodology/approach: The Information Security Culture Change Management (ISCCM) approach is constructed based on literature and the inclusion of the ISCA diagnostic instrument. The ISCA diagnostic instrument statements are also presented in this paper. The ISCCM approach using ISCA is illustrated using data from an empirical study.

Findings: The ISCCM approach was found to be useful in defining change management interventions for organisations using the data of the ISCA survey. Employees' perception and acceptance of change to ensure information security and the effectiveness of the information security training initiatives improved significantly from the as-is survey to the follow-up survey.

Research limitations/implications: The research illustrates the ISCCM approach and shows how it should be combined with the ISCA diagnostic instrument. Future research will focus on including a qualitative assessment of information security culture to complement the empirical data.

Practical implications: Organisations do not have to rely on or adapt organisational development approaches to change their information security culture – they can use the proposed ISCCM approach, which has been customised from information security and change management approaches, together with the presented ISCA questionnaire, to address information security culture change purposefully.

Originality/value: The proposed ISCCM approach can be applied to complement existing information security management approaches through a holistic and structured approach that combines the ADKAR model, Prosci's approach of change management and the ISCA diagnostic instrument. It will enable organisations to focus on

transitioning to a positive or desired information security culture that mitigates the risk of the human element in the protection of information.

Keywords

Information security culture, ISCA, ADKAR, change management, transformation, questionnaire, human

1. Introduction

The information security culture in an organisation can either contribute to the protection of information or introduce risk. An organisation should change its information security culture to a desired state – one where employees are educated and equipped to comply with policies; where information security is perceived as important; where information is protected throughout its life cycle; and where trust is established with customers through the ways their information is processed.

A planned approach to culture change can enable the workforce to adapt to the change and, ultimately, to change their behaviour (Robbins, Judge, Odendaal & Roodt 2016). However, this is not an easy task as the culture must be managed continuously to prevent the organisation from spending resources on incorrect or outdated assumptions about the organisational culture (Ogbonna 1992), including the information security culture. The success of information protection depends on whether employees are convinced through change management to behave in a secure manner to instil a strong information security culture (Ashenden & Sasse 2013).

In an ideal world, one would prefer to deal with change in a planned manner and not as an accidental occurrence. This would allow for intentional activities that are goal oriented (Robbins et al. 2016) to implement the information security strategy of an organisation. However, organisations are still faced with a lack of mechanisms to adapt to change (Ernst & Young 2015). Social media, cloud computing, big data analytics and new legislation and regulations present organisations with new challenges regarding the management of threats and vulnerabilities from both a technological and a human perspective. While most breaches result from external sources, inside employees account for at least 15% of breaches; another 14% of breaches result from errors made by employees, according to the Verison Data Breach Investigations Report (Verizon 2017). The surveys of PricewaterhouseCoopers (PwC 2016, 2018) confirm that the human element remains a concern, with current (34%) and former (29%) employees representing the largest source of compromise from a people perspective, followed by service providers (22%), former service providers (19%) and suppliers (16%). From a technological perspective, organisations regard malware and phishing as the top two threats, which relate to the human component (Verizon 2017; Ernst & Young 2015). Organisations should aim to use planned mechanisms for change to effectively adapt to change and to manage the risk from a human perspective. This also applies to change in information security culture.

The aim of this research is to propose an approach for information security culture change management that specifically includes an as-is diagnostic instrument and to illustrate the implementation of such an approach using data from an empirical study. Such an approach could contribute to fostering a positive information security

culture. In order to achieve the research aims, the Information Security Culture Change Management (ISCCM) approach is proposed. This approach combines concepts of Prosci's ADKAR change management model and approach (Hiatt 2006), the change management concepts of Lewin (1951) and the Information Security Culture Assessment (ISCA) diagnostic instrument (Da Veiga & Eloff 2010; Da Veiga & Martins 2015a, 2015b, 2017). The ADKAR change management model is used as a formal approach to change management in organisations and includes five distinct phases, namely awareness (of the need for change), desire (to support and participate in the change), knowledge (of how to change), ability (to implement the change) and reinforcement (to sustain the change). These phases correlate with the change concepts of Lewin and are used in this research as the foundation of the proposed approach that incorporates ISCA as an as-is diagnostic instrument.

Organisations across industries and of various sizes can use the ISCCM approach and related ISCA. Stakeholders such as Chief Information Officers (CIOs), Information Security Officers (ISOs) and security management teams in organisations can use ISCCM, incorporating ISCA, to complement the organisations' information security programmes. It will provide them with a common and shared understanding of the approach that must be followed for information security culture change, how to conduct the as-is assessment using ISCA, and how to use the data to define and implement actions to transform the culture. ISCCM complements existing approaches to information security management such as the Control Objectives for Information and Related Technologies (COBIT) (ISACA 2007) and ISO/IEC 27002 (ISO/IEC 2013) by incorporating the human element and a way in which to assess and transform the information security culture. This approach compliments traditional information security assessments to include the concept of information security culture using a formally defined approach. The outcome of ISCCM can be used together with internal and external audit reports, monitoring reports, self-assessments, and breach and incident management reports to understand the as-is information security environment from a human perspective and to define improvement plans holistically. This could, for example, assist management in developing information security training and awareness programmes that are not based on outdated assumptions, but on the as-is situation. It will enable management to allocate resources effectively, to prioritise high-risk business areas and to monitor the success and impact of interventions through follow-up assessments. It will also help management to implement initiatives purposefully from a wider perspective in order to create an aspiration for change and to reinforce the changes continuously through a variety of efforts. Academia can use the ISCCM approach as a point of reference for changing information security culture and expand it to incorporate other research methods such as qualitative assessments and case studies across different industries. Academia can further use and customise the ISCA across countries and industries to aid in understanding the as-is information security culture across organisations and how to monitor the change through follow-up assessments.

The remainder of the paper is structured as follows: Section two gives an overview of information security culture and section three discusses existing information security culture approaches that incorporate concepts of change management. This is followed by a discussion of change management approaches from a social sciences perspective, which is used as a point of reference for proposing the ISCCM approach. The ISCCM approach is discussed in section five. The research methodology is discussed in section six, after which the ISCCM approach is illustrated in section seven, using the empirical data of ISCA. Following the discussion and an outline of the limitations, a conclusion is reached in section ten. The ISCA questionnaire is presented in Appendix 2.

2. Information security culture

> *Information security culture is the "attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organisation's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour evident in artefacts and creations that become part of the way things are done in the organisation to protect its information assets." (Da Veiga & Eloff 2010:196–197)*

Information security culture is a subculture of organisational culture (Schlienger & Teufel 2003; Van Niekerk & Von Solms 2005). It refers to the way things are done in an organisation when employees process information, which becomes part of the culture in the organisation (Da Veiga & Martins 2015a). This culture can therefore be explained as the shared meaning that the members of an organisation have about the protection of information and thus of information security as adapted from the explanation of organisational culture (Martins & Martins 2016). Their shared meaning will relate to the manner in which they perceive information security requirements in the organisation and how they need to comply with those requirements. Employees from different departments, job levels, age groups, racial groups or gender groups, each with their own background and diversity traits, will have a common perception and thus a similar information security culture (Martins & Martins 2016). This will result in subcultures of information security across the organisation such as a departmental culture based on shared assumptions or a professional culture based on the qualifications and training of employees (Jex & Britt 2008; Da Veiga & Martins 2017). Each group will have a common perception of the information security requirements of the organisation, that is to say, what they can and cannot do when processing information (Da Veiga & Martins 2017). The dominant information security culture is prevalent in the majority of the employees' perception of upholding the core information security characteristics of the organisation. This dominant information security culture can influence employee behaviour (Martins & Martins 2016) and direct their actions in line with information security policies and expected behaviour.

The information security culture in an organisation develops as a result of the day-to-day behaviour that is exhibited by employees and is visible in artefacts, espoused values and shared tacit assumptions (Schein 1985, 2006). On an artefact level, the expected behaviour is visible in the form of tangible aspects such as an information security policy, information security training, a reporting line for security incidents, regular self-assessments in departments and the technology used by an organisation (Schein 1985; Schlienger & Teufel 2003; Da Veiga & Eloff 2010). The artefact level is underpinned by the values of an organisation, such as customer service or honesty. The shared tacit assumptions, as formed by beliefs and values, relate to how and why employees assume information should be protected when they process it (Van Niekerk & Von Solms 2006; Da Veiga & Eloff 2010). The espoused values form over time and relate to what employees believe should be done to protect information such as not sharing confidential information with third parties to preserve confidentiality and privacy values (Van Niekerk & Von Solms 2006; Da Veiga & Martins 2015b).

A strong or positive information security culture is one where information is protected throughout its life cycle at all points where employees interact with it in some way and where employees have a common perception towards the protection of information in line with the information security policy of the organisation. The interaction of employees with information should be in compliance with the organisation's information security policies and

regulatory requirements. However, the behaviour of internal employees continues to be a concern owing to the number of incidents related to employees in the form or errors, negligence or malicious intentions (Sherif, Furnell & Clarke 2015; AlHogail 2015). Organisations therefore require assistance in directing or changing their information security culture to the desired culture.

3. Existing approaches where change management was applied in the context of information security culture

Detert, Schroeder and Mauriel (2000) identify change management as one of the dimensions of organisational culture, stating that "improvement cannot come without change". Ruighaver, Maynard and Chang (2007) apply the model proposed by Detert et al. (2000) to an organisation's information security culture and incorporate a focus on change. Change management is required in an organisation to improve the compliance of employees with information security polices, the manner in which information is protected and employee awareness, and ultimately to improve the information security culture in the organisation. AlHogail (2015) argues that changing the information security culture in an organisation requires input from management and will result in a huge effort to redirect employees from what they are currently doing wrong.

Research on efforts to redirect employee behaviour in respect of an information security culture ranges from the work that Lewin initiated in 1951 (Ngo, Zhou & Warren 2005; Van Niekerk & Von Solms 2005) to research on the use of change agents (Ashenden & Sasse 2013), change management actions (AlHogail 2015), and the management of different types of changes relating to information technology (Dhillon, Syed & Pedron 2016). The most prominent researchers who have considered the concept of change management in an information security culture are listed in the table in Appendix 1. None of the existing approaches to applying change management or transformational perspectives to an information security culture follow a comprehensive and structured change management approach like ADKAR, neither do they include processes with concrete steps that organisations can apply to redirect and transform their information security culture to a desired state. Recent research on the information security culture in organisations (Connolly, Lang, Gathegi & Tygar 2017; Parsons, Calic, Pattinson, Butavicius, McCormac & Zwaans 2017; Dhillon, Syed & Pedron 2016) also does not include the application of change management approaches in organisations' information security culture that includes an as-is diagnostic instrument that can be used to collect reliable and valid data on which to base the change management decisions.

There are various change management approaches other than Lewin's work that can be considered when developing a comprehensive change management approach for an information security culture. Examples of these approaches include the Congruence Model (Nadler & Tushman 1980), Kotter's Change Model (Kotter 1996, 2006), the Theory of Constraints (TOC) (Patrick 2001; Goldratt 1999; Kazmi & Naarananoja 2014), the Kaizen Model (Plan – Do – Check – Act) (Plunkett & Attner 1994) and Prosci's ADKAR Model and approach (Hiatt 2006). The next section provides an overview of these existing change management models and approaches in order to indicate their positive contributions that serve as the building blocks for an information security culture change management approach.

4. An overview of change management models and approaches

Organisational culture can be understood as "the lens through which employees of an organisation learn to interpret the environment" (Jex & Britt 2008). It will guide employees' behaviour, for instance, to ensure that all access requests are approved and documented, or that all hand-held devices are protected with a password. An organisational culture that has developed over time is difficult to change, mainly because the assumptions of employees might need to change (Jex & Britt 2008). Lewin (1947) introduced the concept of planned change (Boje, Burnes & Hassard 2012). He introduced a three-step approach called "theories of change" (Leban & Stone 2008), where the "unfreezing" step is used to unfreeze existing behaviour through demonstration or clarification of the problem. This is followed by creating a desire to change through driving forces and thus to "move or change" to the desired behaviour, which must be "frozen" again. The *Information security awareness report* published by the Information Security Forum (ISF 2002) lists a number of driving forces and resisting forces that can play a role in this process. The ISF explains the process by using the example of a new policy that requires employees to keep their ID cards with them to enter and exit various areas in a building. Such a rule might be resisted by employees who object to it. By introducing positive driving forces such as canteen discounts for cardholders, employees might realise that they will benefit from adhering to the policy and start to move towards the desired behaviour. This is an effective approach in the context of information security where employees constantly need to adapt to technological changes and where safe habits must be cultivated. Employees' resistance, which is underlined by the organisational culture, needs to be changed to positive acceptance of the change through the use of planned driving forces that are proactively implemented by management (ISF 2002).

In the wake of Lewin's (1951) approach, a number of change management models or approaches have been developed. Nadler and Tushman's (1980) Congruence Model incorporates a focus on organisational performance and the role that leadership plays in the process. They argue that organisations are similar to systems that must be in congruence to ensure optimal performance. In support of the Congruence Model, Nadler and Tushman (1980) propose a process that comprises five stages, namely diagnosis (stage 1), preparation (stage 2), implementing change (stage 3), consolidating change (stage 4) and sustaining change (stage 5) (Leban & Stone 2008). Although their model presents a structured approach, it can involve a long and costly process to implement (Basu 2018).

The important work by Kotter (1996, 2006) outlines an eight-stage change management model that focuses on the processes to follow in institutionalising change:

- establishing a greater sense of urgency
- forming a guiding coalition
- developing a transformational vision
- communicating the transformational vision
- empowering employees to action
- creating short-term wins
- consolidating improvements and producing more change
- institutionalising new approaches in the culture (Kotter 2006; Leban & Stone 2008).

Kotter's (2006) model is designed for a strategic view and is one of the most widely-used models, even though it does not have a tactical focus (Leban & Stone 2008). A critique of Kotter's model is the lack of integration of project management (Kazmi & Naarananoja 2014).

Other models for change management have emerged, for example, Goldratt's (1999) Theory of Constraints (TOC) (Kazmi & Naarananoja 2014) and the Kaizen Model (Plan – Do – Check – Act) (Plunkett & Attner 1994). Arguments against these models are that they are implemented over longer periods and have a longer timeframe of impact (Kazmi & Naarananoja 2014). This critique needs to be viewed in the light of Kotter's work which emphasises that change takes a considerable amount of time, especially when one aims to embed it in the culture of an organisation (Kotter 2006). Other change management models to take note of are those by Kanter, Stein and Jick (1992) and Luecke (2003). These two models incorporate an emphasis on leadership and identifying the need for change (Abdulkadhim, Bahari, Bakri & Ismail 2015). Todnem (2005) critically reviewed change management models in 2005. He did a comprehensive comparison of Kanter, Kotter and Luecke's work as the emerging models, with contrasting views from researchers on the models. Since then new perspectives and models on managing change have emerged. The website of Change Activation lists at least 16 different change management models or approaches for which toolkits are available (Change Activation 2018). Three of the approaches relate to the work of Prosci, which had not yet been developed when Todnem did his review on change management.

The ADKAR Model which was developed by Prosci was published in the form of a textbook in 2006 (Hiatt 2006). In conjunction with the model, Prosci developed a change management approach consisting of three phases, namely preparing for change, managing the change and post-intervention. These three phases correspond to Lewin's (1951) theory, but additional, more detailed steps are embedded in each phase. During phase 1, the change management strategy is defined, the team is prepared and the sponsorship model is developed. In phase 2, the change is managed through management and implementation plans. The ADKAR Model, which serves as a goal-oriented change management model that can be applied in a personal or organisational context, is embedded in this phase. It focuses on the five key areas which make up the acronym ADKAR, namely awareness (of the need for change), desire (to support and participate in the change), knowledge (of how to change), ability (to implement the change) and reinforcement (to sustain the change). The last phase concentrates on post-intervention. In this phase, feedback is collected and analysed, gaps are diagnosed and corrective actions are implemented.

The current state, which must be unfrozen according to Lewin's theory (1951), corresponds to Prosci's awareness and desire phases. The knowledge and awareness phases correspond to a transition to "move or change", as Lewin refers to it. The reinforcement phase aids in refreezing behaviour. These steps are easy to convert to project management plans and focus strongly on employees and changing their behaviour. The approach can be applied to a wide variety of changes, including an information security culture change. From an organisational change perspective, Prosci (2013) finds that eight out of ten projects follow a structured approach to change management which helps them with planned interventions to derive sustainable changes in behaviour. It is therefore necessary, from an information security perspective, to follow a structured approach to changing an information security culture in order to minimise the risk that human behaviour (i.e. error or negligence) could pose to the protection of information.

The ADKAR model can be used effectively to establish whether employees are ready to change. The model can also be used to define corresponding actions plans. Kazmi and Naarananoja (2014) used the ADKAR model as the preferred model in their research on a healthcare project in Finland. They found it effective in identifying problem areas and they adapted it accordingly to implement change effectively and efficiently. The ADKAR model has also been implemented successfully in other scenarios, for example changes to governance structures in a Texas hospital environment (Sheperd, Harris, Chung & Himes 2014) and an analysis of the change management competencies of school heads in Pakistan (Kiani & Shah 2014).

Aspects missing from the Prosci approach and model are how change should be understood from an information security culture perspective, what type of change is required and which information must be gathered prior to the first phase (preparing for change). Information about all these aspects is required to define the strategy, to determine who needs to be involved in the change, to understand the urgency of the change and to develop the aspects needed to address the five areas of ADKAR. The concept of organisational development (OD) can be integrated to address this limitation since it follows an action research design in which a cycle of assessments and evaluations is used to solve a problem (Boje et al. 2012; Berry & Houston 1993; Coghlan & Brydon-Miller 2014). It can be applied to understand the as-is environment from an information security culture perspective and to evaluate the effects of the change by repeating the diagnosis, comparing the results to monitor improvement, and managing and directing the change consistently. This corresponds with the Kaizen Model approach, where an assessment is also conducted as part of the checking phase to ensure continuous improvement.

The next section outlines the proposed information security culture change approach in the light of the above discussion.

5. Information security culture change management (ISCCM) approach

A change management approach to an information security culture should be grounded in existing change management models or approaches since these models have already been used with success in the social sciences. It is furthermore critical to understand the existing information security culture in an organisation before introducing any changes. Therefore, an assessment must be conducted to understand the as-is environment and to determine which behaviours need to change. Once these are understood, it is important to use planned interventions to transform the culture. This requires concrete actions that the organisation can implement to drive the change. Finally, after the interventions, the organisation should reassess whether the actions have had the desired impact and resulted in the desired outcome.

The information security culture change management approach is constructed by incorporating the following aspects from the existing change management approaches discussed in section 3:

- Lewin's theory of "freezing", "moving" and "refreezing" behaviour (which corresponds to ADKAR)
- the ADKAR model, so that the practical implementation of Lewin's theory can be attended to through detailed tactical and operational activities

- Prosci's approach of change management, so that the change management phases can be structured in an organisational change management programme
- the OD process, so that an as-is assessment can be conducted to identify gaps, and so that the rationale for change that can feed into the change management strategy can be defined and the change can be monitored continuously to direct and sustain it

The information security culture change management approach, or ISCCM, is set out in figure 1. It is a holistic approach that focuses on the transition to a positive or desired information security culture in an organisation in order to aid in mitigating the risks posed by the human element in the protection of information. The ISCCM consists of four distinct phases that are implemented on a cyclical basis. Each phase comprises a number of activities as explained below.

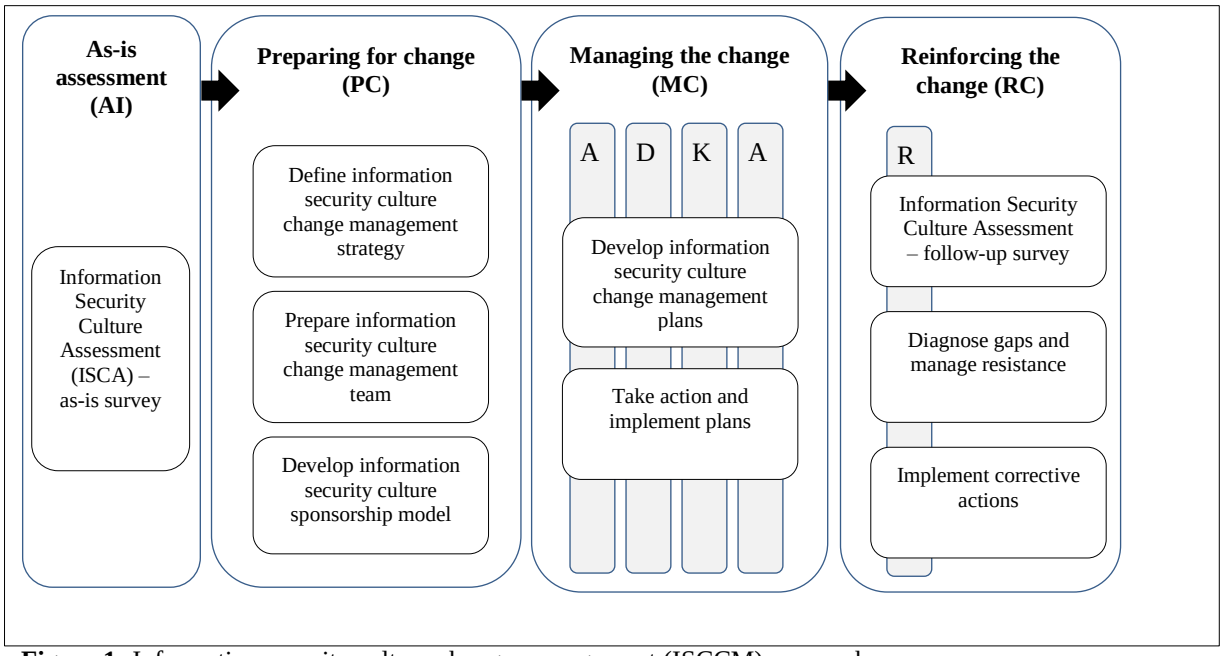

Figure 1: Information security culture change management (ISCCM) approach

5.1 As-is assessment (AI): Before change management activities are embarked on in an organisation, it is essential to conduct an assessment to establish the current situation (Berry & Houston 1993; Byars & Rue 1997; Herold 2011). During this phase, the information security culture level is assessed. This helps the organisation to determine the threats to the information security culture and to identify the strengths in the culture from which to leverage efforts. In essence, the as-is information security culture assessment gives the organisation an indication of the institutionalisation of the information security policy and related requirements. The assessment presents the organisation with a view of what employees perceive and whether it is acceptable or requires intervention. In summary, the as-is assessment presents the organisation with a snapshot of where it is in order to help it determine where it should be.

5.1.1 ISCA diagnostic instrument

The *Information Security Culture Assessment (ISCA)* is used as the key diagnostic instrument (questionnaire) in the as-is assessment (Da Veiga & Martins 2015). Other information security culture diagnostic instruments such

as the diagnostic instruments proposed by AlHogail (2015) and Schlienger and Teufel (2003, 2005), which are offered in a commercial context (Tree Solution 2018), are also available to measure information security culture. These instruments all focus on the information security culture in an organisation, but their perspectives differ. The diagnostic instrument of Da Veiga and Martins (2015) is based on a theoretical model of information security culture (Da Veiga & Eloff 2010), has been customised for the industry, and has been validated through statistical methods with a reliability score of between 0.764 and 0.877 (Da Veiga & Martins 2015b). It provides valid and reliable results over time to facilitate changes in employee attitude and related behaviour, and to inculcate a positive information security culture. Appendix 2 includes the statements of the ISCA diagnostic instrument as customised for the organisation in this study.

The ISCA is conducted in the form of an electronic survey that is distributed to all employees in the organisation to complete. Focus groups are also used to confirm the results of the assessment. Empirical data is derived from the ISCA to understand the level of information security culture in the organisation, the required content of training and awareness programmes, and the stakeholders that need to be prioritised for interventions based on their perceptions.

The ISCA questionnaire consists of three sections:

- A section with information security background questions that are mainly answered using a yes/no scale. This section is developed with the organisation participating in the study to ask questions about the existing policies and awareness activities for background purposes.
- The second section comprises ten dimensions with a total of 55 statements that measure the information security culture on a five-point Likert scale (strongly disagree, disagree, unsure, agree, strongly agree). The ten information security culture dimensions were reduced to six dimensions with 49 statements following the factor and item analysis (Da Veiga & Martins 2015b).
- A biographical section is included. Participants are required to answer demographical questions to segment the data in employee groups such as office location, generation group, gender, business unit and/or job level.

5.1.2 Overall information security culture mean

The means for the ten dimensions and for the various demographical groups are determined. The lowest and highest items are identified per demographical group to identify focus areas for change management activities. When the analysis of variance (ANOVA) test reveals that specific biographical groups are significantly more negative than the other groups, these groups are regarded as high-risk groups. Action plans for these groups can be prioritised as part of the ISCCM approach. Further statistical analysis is conducted to identify recommendations for improvement which can be included in the change management strategy.

To supplement the ISCA results and draw correlations, other metrics such as monitoring, compliance audits, internal and/or external audits, incident management data and risk assessment outcomes can be used to obtain a holistic view of information security implementation and controls in the organisation. Owing to the statistical

validity and reliability of the ISCA diagnostic instrument, it was selected for inclusion in the ISCCM to understand the as-is information security culture and to monitor the change over time.

5.2 Preparing for the change (PC)

The as-is diagnosis aids in defining the need for change. The information security culture change objectives are derived from the outcomes of ISCA and feed into the *information security culture change management strategy*. The strategy can vary depending on the nature of the outcome of the as-is assessment. This implies that the strategy might involve minimal intervention in some cases and comprehensive interventions in other cases to protect the organisational data and to create a competitive advantage while mitigating the risks. The strategy could address aspects such as the improvement of the information security culture and compliance as identified in the ISCA data.

Since culture change takes many years, the strategy should also span a number of years and incorporate continuous assessment. Rossouw and Van Vuuren (2013) refer to four broad strategies for the management of ethical culture, namely "reactive, compliance, integrity and totally aligned" strategies. In the context of the information security culture in an organisation, a reactive strategy is prevalent when management aims to address information security after breaches and incidents have occurred without proactive intervention such as educating and training employees. A compliance strategy focuses on aligning employee behaviour with the information security policies, whereas an integrity strategy focuses on the strategic advantage of a strong information security culture and not only on minimising incidents. The ultimate strategy to aim for is the totally aligned strategy, which means that the information security culture is embedded in the organisation's strategy and vision, and positive behaviour is rewarded as part of the culture.

Once the strategy has been defined, the resources required for the project are identified. Resources could include internal teams, external consultants and/or third parties. A *change management team* is established with key stakeholders from across the business who can assist in rolling out the implementation and act as change agents.

Lastly, the *information security culture sponsorship model* is defined to identify the leaders in the organisation and the management roles that will be involved in supporting and sponsoring change management initiatives. Leaders play an important role in directing change and behaviour (Jex & Britt 2008). Similarly, top management plays a role in the development of the culture in an organisation (Martins & Martins 2016). If change in culture is required, top management must become involved in and support the change, and lead by example to promote employee buy-in.

5.3 Managing the change (MC)

Information security culture change management plans are developed based on the strategy and the findings of the as-is diagnosis using the ISCA diagnostic instrument. The plans are developed according to the ADKAR phases to implement driving forces and to change behaviour to the desired state when *the action plans are implemented*. Although ADKAR focuses on areas that must be developed or changed, it is essential to approach the activities from a project management perspective. This means that roles must be allocated, deadlines defined

and progress monitored during the development and implementation phases. Approaches such as Project Management Body of Knowledge (PMBOK), Gantt charts or work breakdown structures can be followed (Whitman & Mattord 2017).

The ISCA data is specifically used in the awareness and knowledge phases of ADKAR. In the awareness phase the need for change becomes evident when the ISCA dimensions and/or statements with the most negative scores on the mean are considered. Awareness can then be created about the concepts identified. If, for example, employees feel that the information security policy is too difficult to understand, management can be made aware that there is a need to change or update the information security policy to make it more understandable. During the knowledge phase, developmental dimensions and statements identified in the ISCA serve as input to define the topics that should be included in the creation of awareness. In this way, specific topics can be prioritised and targeted for specific demographic groups identified in the data. For example, the background questions in the ISCA are used to determine if employees have read the information security policy and the information security culture question is used to determine if the policy is understandable.

A desire to participate in and support the change and the ability to implement the change are not necessarily dependent on the ISCA data, but on the involvement and buy-in of management, project management and the available resources in the organisation. The ISCA data can be used as motivation to create a desire for change and to define the acceptable mean score for the ISCA dimensions.

5.4. Reinforcing the change (RC)

As part of the feedback process, the change management team needs to establish whether employee behaviour has indeed changed. This can be done by defining measurement criteria for desired outcomes. Similarly, audits, quality control or compliance testing can be used to confirm whether all access to a system has been authorised, for example. Technology can be used to determine how many hours employees spend on the internet and whether employees back up information to the designated file servers. Where gaps are identified, the message can be reinforced, positive behaviour can be rewarded and incorrect behaviour can be followed up.

A *follow-up ISCA* is conducted to establish whether the implemented change management actions have had a positive impact on the information security culture. A follow-up ISCA also enables the organisation to determine whether the change management activities have been successful from a culture perspective and whether other developmental areas have arisen over time. Data from a follow-up ISCA survey for a specific organisation facilitates the successful monitoring of the culture change over a period of time. Data from the as-is assessment and the follow-up ISCA is compared to identify trends and improvements (or areas where there has been a decline). Any dimensions or statements that have not improved since the as-is assessment can be regarded as *gaps*, for which *corrective actions* are defined and implemented. The messages and changes are reinforced based on the last phase of ADKAR through various activities or repetition such as monthly e-mails, online training, change agents and face-to-face discussions.

The research methodology section sets out the application of the ISCCM approach with ISCA in an organisation to illustrate its implementation.

6. Research methodology

6.1 Research design

The research was done in the form of a quantitative study in an organisation. The ISCCM is illustrated using data from an ISCA that was conducted at two intervals in a financial organisation. The organisation conducted the information security culture assessment to monitor the success of its information security programme, to identify where to focus training and awareness initiatives and, ultimately, to determine what to change in order to instil a positive information security culture.

6.2 The organisation

The empirical study was conducted in the offices of the organisation and which are located in 12 countries. The Group Information Security Officer (GISO) of the organisation manages information security with a team of Country Information Security Officers (CISOs) and Business Unit Information Security Officers (BISOs). Information security is managed via a formal programme in the organisation through regular awareness and training initiatives. Offices across all the countries have to adhere to the group's information security policies and procedures. This research study was conducted as part of an information security culture assessment to monitor changes in the organisation's information security culture after the implementation of corrective actions.

6.3 Responses

The census sampling method (Cooper & Schindler 2003:179) was used for the empirical study and all employees in the organisation were included in the survey invite. The survey link was e-mailed by the organisation to all its employees at all job levels in all its offices in the different countries. A competition was included in the survey. To enter the competition, employees had to supply their e-mail address when they submitted the survey. They then stood a chance of winning one of a number of iPads. To protect the employees' privacy and to maintain confidentiality, e-mail addresses were separated from survey responses and all duplications were removed.

The survey was conducted at two intervals with a timeframe of three years in between. At the time of the first survey, the organisation employed +/- 7 000 employees, of whom 2 320 responded to the survey. During the follow-up survey, the organisation employed +/- 8 000 employees, of whom 2 159 participated in the survey. Since employees participated on a voluntary basis, the method proposed by Krejcie and Morgan (1970) was applied to determine the minimum number of responses required for a 95% confidence level. For the as-is survey, a total of 364 responses was required and for the follow-up survey, a total of 367 responses was required, comprising a 33% response rate for the as-is survey and a 26% response rate for the follow-up survey. The difference in the response rates can be attributed to the voluntary nature of the survey. For both surveys, an adequate number of responses was received for the overall data to be generalised to the overall population at a 95% confidence level.

SurveyTracker (Scantron 2018) and IBM SPSS Statistics Version 22.0 (IBM 2011) were used to conduct the statistical analysis. The data was analysed, and the means, the frequencies and the frequency distribution were

determined for the overall data and biographical segmentation. ANOVA and t-tests were used to determine the significant differences between the biographical groups in order to prioritise change management initiatives. Biographical groups with less than five responses were not included in the analysis in order to protect the respondents' confidentiality.

7. Application of the ISCCM approach using ISCA

Data from the as-is survey was used to define change interventions following the ISCCM approach. The as-is data was compared with the follow-up data to establish whether the organisation had made progress with the development of the desired information security culture. The participating organisation implemented comprehensive action plans following the as-is survey based on the ISCA findings.

The discussion below outlines how the ISCCM was applied in the context of the participating organisation.

7.1 As-is assessment (IA)

The data of the as-is survey was used to obtain an understanding of the as-is information security culture of the organisation. The information security culture means for half of the dimensions were below 4.00. The cut-off for improvement, as agreed with management, was 4.00 for the mean (Da Veiga & Martins 2015). Therefore, the information security culture means of five of the dimensions could be improved through specific interventions. The privacy perception (3.56), training and awareness (3.02), information security leadership (3.88), trust (3.88) and information security programme (3.96) dimensions had the lowest mean scores and were thus identified as the priority dimensions to focus on (see table 1).

Table 1: Information security culture dimension means and percentage agree scores for the as-is and follow-up surveys

Information security culture dimensions	As-is survey means	% agree	Follow-up survey means	% agree	Improvement
1. Change management	4.09	84.7%	4.14	86.1%	Yes
2. Information asset management	4.22	88.9%	4.30	91.2%	Yes
3. Information security leadership	3.88	76.1%	4.03	82.1%	Yes
4. Information security management	4.14	90.6%	3.96	80.1%	No
5. Information security policies	4.08	80.5%	4.15	82.5%	Yes
6. Information security programme	3.96	76.8%	4.05	80.5%	Yes
7. Trust	3.88	74.8%	3.95	76.8%	Yes
8. User management	4.08	83.4%	4.14	85.8%	Yes
9. Training and awareness	3.02	39.9%	3.08	43.0%	Yes
10. Privacy perception	3.56	61.5%	3.67	65.4%	Yes

The most negative statements in the prioritised dimensions were identified to develop specific interventions. Table 2 provides an extract of some of the negative statements in these dimensions and the corresponding mean and percentage agree scores for both surveys. The offices with the lowest mean scores for each statement are also

included in table 2. These can be regarded as high-risk offices that must be prioritised for the implementation of action plans.

Table 2: The most negative IS culture statements and improved scores

Most negative culture statements – as-is survey	Dimension	Mean		% agree		Lowest office % agree – based on as-is survey	
		As-is survey	Follow-up survey	As-is survey	Follow-up survey	As-is survey	Follow-up survey
21. I believe X's employees adhere to the information security policy.	Information security leadership	3.66	3.81 **	65.4%	72.8%	SA – PE 38.1% SA – Jhb 52.5% Australia – 62.9%	SA – PE 80% SA – Jhb 63.7% Australia – 74.7%
20. My division clearly outlines what is expected of me with regard to information security.	Information security leadership	3.66	3.82 **	68.2%	73.5%	Australia – 52.3% UK – Abingdon – 56.7% SA – Jhb – 59.2%	Australia – 68.3% UK – Abingdon – * SA – Jhb – 68.2%
38. I believe that third parties who have access to confidential information preserve its confidentiality.	Trust	3.38	3.50 **	44.8%	49.7%	SA – PE 28.6% Switzerland – Zurich 33.3% SA – Pretoria 36.4%	SA – PE 36% Switzerland – Zurich 66.7% SA – Pretoria 40.7%
33. I believe my division commits enough people to information security.	Information security programme	3.60	3.77 **	56.5%	64.9%	SA – PE 42.9% UK – Abingdon 43.3% SA – Jhb 47.8%	SA – PE 64% UK – Abingdon * SA – Jhb 58.1%
34. I believe my division commits enough money to information security.	Information security programme	3.59	3.70 **	53.6%	59.1%	SA – PE 38.1% Switzerland – Zurich 38.9% SA – Jhb 44.5%	SA – PE 68% Switzerland – Zurich 73.3% SA – Jhb 56.1%
32. I believe my division commits enough time to information security.	Information security programme	3.66	3.82 **	63.9%	72.2%	SA – PE 57.1% SA – Cape Town 58.5% Australia 59.0%	SA – PE 80% SA – Cape Town 71.0% Australia 75.3%

Note: *UK – Abingdon office not included in follow-up survey

** Significant difference, indicating an improvement, between as-is and follow-up survey as per t-test Sig. (2-tailed) value was 0.000 for the means (significant if $p < 0.05$) (Howell 1995)

The offices with the lowest overall mean score in the as-is survey were UK – Abingdon (3.92), Australia (3.93) and SA – Jhb (3.96). The gaps in the information security knowledge section related to only 61.6% (lowest scored offices: SA – Pretoria 45.5%; SA – Durban 49.4%; UK – Abingdon 50%) of employees, who indicated that they had read the information security policy. Only 67.8% (lowest scored offices: Australia 51.1%; UK – Abingdon 51.7%; UK –Manchester 62.5%) knew where to get a copy of the information security policy. Furthermore, only 38.7% of employees knew who their business unit security officer was, while 48.2% knew who the group information security officer was. The Zurich office (55.6%) and the Ireland office's (40.8%) employees knew of more information security breaches compared to, for example, SA – Durban, with only 2.6%, and Australia, with 3.5%. No significant differences were found between the job levels and, as such, the interventions were not tailored to job levels, but rather to office locations where significant differences were identified.

The organisation's employees had a very positive view of change management. Ninety-five per cent of employees indicated that they accepted that some inconvenience was necessary to secure important information. An

additional 95.1% indicated that they were prepared to change their working practices in order to ensure the security of information assets, while 80.1% felt that their division positively accepted changes in their working practices in order to ensure the security of information assets. These aspects are positive building blocks that can be used to leverage the change management strategy and to introduce change to employees. Employees indicated that their preferences for receiving information security messages were via e-mail (86.3%), presentations (26.5%) and the intranet (15.5%). These methods can be incorporated in the change management plan.

7.2 Preparing for change (PC)

In preparation for change, a broad strategy was formulated to improve the information security culture in the organisation. The strategic initiative of the organisation was defined as focusing on improving information security leadership to create a trusting environment where the information security programme could function effectively and efficiently to aid in fostering a strong information security culture. Over time, management envisaged a culture in which the overall mean and the individual dimension means of the information security culture would be above 4.00, aiming for a totally aligned information security culture. From a behavioural perspective, management envisaged a culture where employees would comply with information security policies and understand what was expected of them to protect information at all times. A change management team consisting of the GISO and related CISOs and BISOs was established. The organisation included external consultants as part of the team to assist in developing the outputs of the defined action plans and initiatives. The GISO acted as the project sponsor and coordinated the project.

7.3 Managing the change (MC)

This section outlines how the results of the ISCA were used to compile a change management plan using ADKAR in the MC phase. The first ISCA served as the as-is assessment to create awareness and a desire to change as part of the current phase relating to the awareness and desire phases of ADKAR. The action plans defined on the basis of the as-is data were implemented, leading to the transition phase, which, in turn, map to the knowledge and ability phases of ADKAR. The follow-up ISCA allowed for a comparison between the data to establish whether there was improvement or change, resembling the reinforcing phase of ADKAR. The ISCA data was used as follows in the MC phase:

Awareness: In the awareness phase of the ADKAR model, the ISCA data is used to motivate why change is necessary. In the participating organisation, the researchers participated in presenting the findings to the project team and a CISO presented the findings to the various stakeholder groups. During the presentation, the findings, the impact of a negative culture, and breaches and incidents that further justified why change was necessary were discussed. An overview of the key findings was communicated to employees of the organisation. The top ten statements and bottom ten statements needed to be prioritised since they would guide the priority of action plans. Priority offices, as identified in the demographical groups, also needed to be communicated to initiate and focus on interventions with the most critical groups. In the case of the participating organisation, the Abingdon,

Australia and Johannesburg offices scored the lowest and were therefore prioritised in terms of creating awareness and implementing focused action plans.

Desire to change: In the desire-to-change phase of ADKAR, the desired outcome is depicted. In the case of the participating organisation, the desired outcome was to achieve improved mean scores for the information security culture dimensions. A key action that can support this is to conduct focus groups to obtain the commitment and buy-in of management. As part of the focus groups, the desire for change can be created by discussing the positive impact of leadership and governance in information security. Furthermore, competitions can be considered, for example the nomination of role models for information security or prizes for departments with zero information security incidents per month. In addition, certain information security compliance aspects can be incorporated in employee performance appraisals. In the participating organisation, a number of focus groups were conducted and meetings were held with key stakeholders to aid in creating a desire for change.

Knowledge: During the knowledge (transition) phase, employees are provided with the knowledge required to change. The ISCA data is used to define the knowledge areas or topics to create awareness or training. In the case study, some of the priority topics related to policy compliance (statement 21), expectations (statement 20), third parties (statement 38), commitment (statements 32, 33 and 34) and the location of the information security policy (knowledge section). Awareness and training material was created for the priority topics, to be disseminated using the preferred methods of communication. The following specific methods were implemented by the participating organisation: monthly awareness e-mails, group presentations, annual induction training presentations, a brochure with a summary of information security policy requirements to mail to all, and the creation of an information security portal on the intranet with information security policies, updates and messages.

Priority audiences can be identified, and tailored awareness or training initiatives can be developed on the basis of the developmental aspects identified for those audiences. The following aspects were defined for the participating organisation:

- Creating awareness regarding third-party compliance with data protection policies among internal staff and third parties, prioritising SA – PE, Switzerland – Zurich and SA – Pretoria.
- Communicating the location of the information security policy and procedures, with a focus on Australia, UK – Abingdon and UK – Manchester.
- Communicating the commitment from the organisation to invest in people, time and money to implement information security requirements, specifically in relation to SA – PE/Jhb/CT, UK – Abingdon, Switzerland – Zurich and Australia.
- Summarising the requirements of the information security policy and creating awareness about it, focusing on Australia, UK – Abingdon and SA – Jhb.
- Creating awareness about the requirements for compliance and the consequences of non-compliance among all staff.
- Communicating who the information security officers are in the group and in the business units to all employees.

Ability to change: To enable the organisation to change, CISOs and BISOs can be trained, as was done at the participating organisation. In addition, change agents can be appointed in high-risk offices to assist with the identified interventions, unless the CISOs and BISOs fulfil this role as in the participating organisation. Additional information security officers can also be appointed in large offices such as the UK – London and the SA – Jhb offices. External consultants can be used to assist with the roll-out of the action plans. The ability to change can be strengthened though activities such as awareness sessions, spot checks, brown bag sessions and self-assessments in the business units to determine compliance with information security policies. The participating organisation specifically focused on training the CISOs and BISOs, as well as awareness sessions and self-assessments.

7.4 Reinforcing the change (RC)

The changes that are implemented in the MC phase are reinforced in the RC phase through a follow-up assessment of the ISCA survey to monitor the changes and to benchmark the results. In the case study, nine of the ten information security culture dimensions improved, as indicated in table 1. The mean of the information security management dimension was lower, which could be attributed to the structural changes that took place before the follow-up survey. Employees' perceptions of their divisions' positive acceptance of change to ensure the security of information assets improved significantly from 80.1% to 85%, as indicated by the t-test results. Employees also indicated that the effectiveness of training had improved significantly, from 66.1% to 69.4%. Forty-one of the 55 statements in the culture section improved significantly according to the results of the t-tests (see the extract in table 2 indicated by **). The data indicates that the information security culture became more positive over time. One of the reasons for this relates to the comprehensive action plans that were implemented after the as-is assessment to address identified developmental aspects. A stronger information security culture relates to an improvement of the perception of employees regarding the protection of information. It therefore illustrates an improved common understanding of information security and a positive attitude towards the protection of information across the organisation. To determine whether information security incidents and breaches were lower, the data in an information security breach report could have been reviewed and audit reports could have been used in triangulation to support the results. However, such information was regarded as confidential by the organisation and therefore could not be shared with the researchers. However, from the survey data, the researchers could, for example, establish that employees knew that fewer passwords where shared (as-is survey: 16.3%; follow-up survey: 13.5%) and that more employees read the information security policy (as-is survey: 61.1%; follow-up survey: 64.1%). This supports the findings of an improved information security culture based on the perceptions of employees.

To further reinforce the change, the participating organisation implemented an annual awareness campaign by sending out e-mails and messages on the information security portal in line with developmental aspects identified in survey and priority offices. The organisation also conducted quarterly face-to-face discussions in the various offices about information security requirements and/or changes.

8. Discussion

Information security officers have to implement information security programmes to protect the integrity, availability and confidentiality of organisational information. Organisations can use various international standards to manage information security in order to protect information. These standards include ISO/IEC 27002 (ISO/IEC 2013), COBIT (ISACA 2007), The Standard of Good Practice for Information Security (SOGP) (ISF 2007), the National Institute of Standards and Technology's (NIST) Handbook (NIST 2015) and technical standards like those outlined in the PCI DSS requirements and security assessment procedures (Version 3.2) (PCI Security Standards Council 2016). However, managing employees' behaviour and interaction with information in the context of information security is a challenge that is not addressed by information security management standards. The ISCCM approach can complement these standards by providing an organisation's management with a planned and focused method according to which they can implement a strategy intentionally to achieve higher levels of compliance with policies and to mitigate information security incidents related to employees' errors or negligence. This is achieved by focusing on the high-risk or priority employee groups and information security concepts identified in the ISCA survey, tailoring and implementing interventions through a phased approach to embed change using an approach such as ISCCM.

The ISCCM approach serves as a comprehensive and structured change management approach consisting of concrete phases that organisations can apply to redirect and transform their information security culture to a desired state. It could aid in transforming the information security culture in an organisation through a planned approach. Whitman and Mattord (2017) argue that information security awareness and training can change employee behaviour that hinders the protection of information; however, raising awareness and providing training will not be effective if the interventions do not focus on the correct messages and do not target the developmental areas. An advantage of the ISCCM approach using ISCA for the as-is phase is that by identifying high-risk groups (e.g. certain office locations, job levels or generation groups), resources (e.g. people, time and money) can be focused and efforts directed towards implementing specific and tailored interventions, as opposed to investing resources on generic awareness programmes targeting the entire workforce. Another benefit of this approach is that management can obtain insight (that is not based on assumptions) into employees' perceptions of information security on different levels in the organisation. Benchmarking the results by way of a follow-up survey shows management whether the initiatives have been successful and where they should invest in the future to reinforce their messages to employees. Instead of only focusing on knowledge creation by raising awareness and offering training programmes, management can incorporate initiatives to create a desire to change in employees and to equip them thereby embedding the changes in the long term.

The application of the ISCCM approach can have a positive impact on the information security culture in an organisation and can have successful change outcomes. The ISCCM approach addresses some limitations of existing change management approaches since it incorporates a tactical and operational focus during the implementation of the plan and is cost-effective because it is based on a survey. The incorporation of the ISCA survey makes the ISCCM relevant to information security because information security perceptions of employees are assessed with the aim of transforming the culture.

9. Limitations

The discussion of the ISCCM approach in this study includes a quantitative assessment using ISCA for the as-is survey in the AI phase following a quantitative approach. Other organisational data or reports and qualitative data were not used, but they could be incorporated to validate and complement the as-is survey results of the AI phase and the follow-up survey results of the RC phase. This ISCCM approach incorporating the ISCA diagnostic instrument has only been implemented in one organisation. It can be expanded to more organisations across industries to compare the results regarding the culture change and the impact of transformation.

10. Conclusion

There is limited work that focuses on formal information security culture change approaches to transform the information security culture of organisations to the desired state. In this research, the work of Prosci relating to the ADKAR model was integrated with the ISCA diagnostic instrument to propose an information security culture change management approach. The statements of the ISCA diagnostic instrument were specifically included to inform future research aimed at implementing and improving the approach. The application of this approach was illustrated through an empirical study conducted in a financial organisation.

The ISCCM approach was applied to illustrate how interventions are developed on the basis of data obtained through the ISCA diagnostic instrument to create a desire among employees to change and to reinforce the change with a follow-up survey to monitor the change after the identified actions have been implemented. The overall phases of the ISCCM, namely the establishment of the current situation, the transition and the future state, and the activities in the ADKAR phases were discussed. The survey data was segmented to identify and prioritise high-risk demographical groups for interventions to inform the action plans in the ADKAR phases. Certain offices of the participating organisation were identified as high-risk areas based on the low mean score on dimensional and individual statement levels. The overall mean of the information security culture improved from the one survey to the next, with significant improvements on an individual statement level and for the offices.

The ISCCM approach serves as a structured approach that combines elements of ADKAR and ISCA to direct efforts to change the information security culture in an organisation in order to minimise incidents related to human error or negligence when employees process information. This assists management, for example, in developing information security training and awareness programmes that are not based on outdated assumptions, but on the as-is situation. It enables management to allocate resources effectively, to prioritise high-risk business areas and to monitor the success and impact of interventions. It helps management to implement initiatives purposefully from a wider perspective in order to create an aspiration for change and to reinforce the changes continuously through a variety of efforts.

The ISCCM approach can be improved by incorporating qualitative assessment methods to identify issues in a specific context. Further research can focus on applying the ISCCM approach in other industries and testing the effectiveness of the approach over time. Changing a culture could take many years, but by applying a structured approach such as the ISCCM approach, organisations can purposefully transform their information security culture to a desired state where employee behaviour is in line with organisational policies and requirements for protecting information.

Appendix 1: Information security culture change management research

Author	Concepts			Summary
	Concept of change	Framework or model for change	Quantitative as-is assessment	
Haydon (2016)	Yes	No	Yes	A security culture diagnostic survey to transform the culture in an organisation to a desired culture. Lance Haydon published a book that focuses on a people-centric approach to transforming the security culture of an organisation. He developed a security culture diagnostic survey (SCDS) consisting of ten questions to diagnose the current culture and proposed a method to analyse and interpret the data with the objective of transforming the existing culture to a desired culture.
Dhillon, Syed and Pedron (2016)	Yes	No	No	An organisational transformation case study. This study examined the forming of an information security culture during a merger in a case study organisation using interviews. The findings relate to formal, information-related and technical changes, among other things, and what management should focus on to institutionalise changes. A framework for change and an as-is diagnostic instrument was not developed as part of the study to gather quantitative data.
AlHogail (2015); AlHogail and Mirza (2014)	Yes	No	Yes	An information security culture framework. In this research, AlHogail proposes an information security culture framework incorporating change management, together with ten focus areas, namely training; focus groups; change agents; motivation; milestones and measures; involvement; management support; resources; communication; and culture assessment. Although an information security culture framework was developed, the research does not extend to a framework for change.
Ashenden and Sasse (2013)	Yes	No	No	CISOs as change agents. The researchers propose that Chief Information Security Officers act as change agents and understand their role to make an impact on the information security culture in organisations. The research does not extend to a framework or an as-is diagnostic instrument.
Lacey (2010)	Yes	No	No	A discussion of theory. Lacey concentrates on information security awareness programmes and how they can be used to change the information security culture in organisations. The research does not extend to a framework or an as-is diagnostic instrument.
Van Niekerk and Von Solms (2005); Okere, Van Niekerk and Carroll (2012)	Yes	Yes	No	An outcomes-based framework for culture change. The researchers incorporate the transformative change steps of Lewin (1951) (unfreezing/learning/refreezing) to compile an outcomes framework for culture change. The proposed framework incorporates a step where an assessment of the current culture is conducted and the ideal future state is defined. The gap serves as input to activities to educate employees. Finally, metrics are defined to monitor and maintain the culture. The as-is diagnostic instrument it not included.
Ruighaver, Maynard and Chang (2007)	Yes	No	No	An information security culture model with a focus on change. The researchers apply the model developed by Detert et al (2000) to propose an information security culture model that includes a focus on

Author	Concepts			Summary
	Concept of change	**Framework or model for change**	**Quantitative as-is assessment**	
				change and innovation. The research does not include a change management framework or an as-is diagnostic instrument.
Ngo, Zhou and Warren (2005)	Yes	Yes	No	An information security culture transitional model. This research proposes a transitional model for an information security culture and bases it on the model developed by Bridges (2003). It consists of three phases, namely ending (activities to end the old culture), neutral (the process of moving to the new culture where requirements are put in place) and new beginning zone (reinforcing the new culture) in which change activities are grouped. These phases are in line with the work of Lewin (1951). The research does not extend to the development of an as-is diagnostic instrument.
Schlienger and Teufel (2003, 2005)	Yes	No	Yes	An information security culture questionnaire to measure the as-is culture and transition to the desired culture. Schlienger and Teufel (2003, 2005) developed a questionnaire focusing on 12 dimensions to measure information security cultures. They also developed an online tool that employees can use to complete the questionnaire. The tool is used to analyse the data in order to implement action plans to transform the culture. They validate the questionnaire from an academic perspective. The questionnaire is currently available in German as a commercial service to the industry (Tree Solution 2018). Their initial works incorporate the work of Lewin (1951) (unfreezing/learning/ refreezing), but not as part of an information security culture change framework or model.

Appendix 2: Information Security Culture Assessment (ISCA) diagnostic instrument (questionnaire)

The table below outlines the ISCA statements in column one. The original ISCA dimension names are presented in column two and the new dimension names, based on the factor and item analysis, are presented in column three. The background questions relate to questions one to 18, and the ISCA information security culture statements range from questions 19 to 73, which are listed randomly. For the factor and item analysis results, please refer to Da Veiga and Martins (2015b).

ISCA statements	Original ISCA dimensions	New factor name
1. I know what information security is.	Background questions, yes/no scale	N/A
2. I am aware that X has a written information security policy.	Background questions, yes/no scale	N/A
3. I have read the information security policy.	Background questions, yes/no scale	N/A
4. I know where to get a copy of the information security policy.	Background questions, yes/no scale	N/A
5. I know who the group information security officer is.	Background questions, yes/no scale	N/A
6. I know who my business unit security officer is.	Background questions, yes/no scale	N/A
7. I know what my responsibilities are regarding information security.	Background questions, yes/no scale	N/A
8. I know what an information security incident is.	Background questions, yes/no scale	N/A
9. I know of an information security breach within my business area within the last 12 months.	Background questions, yes/no scale	N/A
10. I have been informed of information security requirements in the last six months, e.g. regulations regarding the downloading of e-mail attachments or browsing the internet.	Background questions, yes/no scale	N/A
11. I believe that the sharing of passwords should be used to make access to information easier.	Background questions, yes/no scale	N/A
12. I am aware of colleagues sharing passwords in my environment.	Background questions, yes/no scale	N/A
13. I understand that some documents are more sensitive than others.	Background questions, yes/no scale	N/A
14. I am aware of a business continuity plan in my business unit.	Background questions, yes/no scale	N/A
15. Which of the following could contain confidential information? Please select all that apply: Hard copy documents (e.g. printed reports) Electronic documents Faxes Business discussions Telephone conversations E-mail Voicemail messages Documents saved on a PDA (personal digital assistant) or a mobile phone Instant messaging conversations All the above.	Background question, multiple response scale	N/A
16. With whom do you believe you may share your password? Please select all that apply Helpdesk My manager No one A secretary A colleague	Background question, multiple response scale	N/A
17. To whom should information security incidents be reported? Please select all that apply: The helpdesk My immediate manager Group information security officer Human Resources IT I don't know The whistle-blowing process should be used	Background question, multiple response scale	N/A

ISCA statements	Original ISCA dimensions	New factor name
18. How do you prefer to receive information security messages? Please select all that apply: Intranet Posters E-mail Discussion groups Presentations Hands-on training SMS messaging Web-based training Desk drop Induction training TV or videos Booklets	Background question, multiple response scale	N/A
19. X's information security policy is applicable to me during the execution of my daily duties.	Information security policies	Information security necessity and importance
20. Information security must be managed through a formal programme (e.g. employees have defined information security roles and responsibilities, awareness campaigns).	Information security programme	Information security accountability
21. Executive and senior managers demonstrate commitment to information security.	Information security leadership	Management buy-in
22. I believe my division is protecting its information assets (e.g. computer equipment and documents) adequately.	Information asset management	Management buy-in
23. The contents of the information security policy were effectively communicated to me.	User management	Information security policy effectiveness
24. Our division positively accepts changes in our working practices in order to ensure the security of information assets.	Change management	Management buy-in
25. I believe that third parties who have access to confidential X information preserve its confidentiality.	Trust	Not included
26. The contents of the information security policy are easy to understand.	Information security policies	Information security policy effectiveness
27. I believe it is necessary to commit time to information security.	Information security programme	Information security necessity and importance
28. Managers in my division appear to adhere to the information security policy.	Information security leadership	Management buy-in
29. It is important to understand the threats (e.g. theft of equipment and the alteration or misuse of information) to the information assets in my division.	Information asset management	Information security necessity and importance
30. I believe I have a responsibility regarding the protection of X's information assets (e.g. information and computer resources).	User management	Information security necessity and importance
31. I am informed in a timely manner as to how information security changes will affect me.	Change management	Information security policy effectiveness
32. I believe that X keeps my private information (e.g. salary or performance appraisal information) confidential.	Trust	Management buy-in
33. I believe the information security policy is practical.	Information security policies	Information security policy effectiveness
34. I believe it is necessary to commit people to information security.	Information security programme	Information security necessity and importance
35. My colleagues demonstrate commitment to information security.	Information security leadership	Management buy-in
36. Information security is necessary in my division.	Information asset management	Information security necessity and importance
37. Information security is primarily a technical issue (it involves predominantly the IT division).	User management	Not included
38. I accept that some inconvenience (e.g. changing my password regularly, locking away confidential documents or making back-ups) is necessary to secure important information.	Change management	Information security necessity and importance
39. I believe that X communicates relevant information security requirements to me.	Trust	Information security policy effectiveness
40. I believe information security requirements should be incorporated in my daily duties.	Information security management	Information security accountability
41. I believe it is necessary to commit money to information security.	Information security programme	Information security accountability

ISCA statements	Original ISCA dimensions	New factor name
42. IT employees demonstrate commitment to information security.	Information security leadership	Information security commitment
43. Information assets in electronic media format (e.g. information saved on my hard drive, CDs or a memory stick) need to be protected.	Information asset management	Information security necessity and importance
44. Information assets in paper format/hard copy format (e.g. contracts and printed reports) need to be protected.	Information asset management	Information security necessity and importance
45. I am aware of the information security aspects relating to my job function (e.g. how to choose a password or handle confidential information).	User management	Information security necessity and importance
46. I am prepared to change my working practices in order to ensure the security of information assets (e.g. computer systems and information in paper or electronic format).	Change management	Information security necessity and importance
47. I believe that X implements information security measures.	Trust	Information security commitment
48. Information security should be part of my performance development programme (PDP).	Information security management	Information security accountability
49. I believe my division commits enough time to information security.	Information security programme	Information security commitment
50. Information security is perceived as important by my colleagues.	Information security leadership	Information security commitment
51. I believe my division will be able to continue its daily operations if there is a disaster resulting in the loss of computer systems, people and/or premises.	Information asset management	Not included
52. I am aware of the negative consequences of contravening X's information security policy.	User management	Information security necessity and importance
53. I believe it is necessary for X to monitor compliance with the information security policy.	Information security management	Information security necessity and importance
54. I believe my division commits enough people to information security.	Information security programme	Information security commitment
55. Information security is perceived as important by managers.	Information security leadership	Management buy-in
56. I believe that the information I work with is protected adequately (e.g. access control to buildings and offices, locking away confidential information, awareness of what information I give to other people and log-on credentials needed for access to computer systems).	Information asset management	Information security commitment
57. I believe my division commits enough money to information security.	Information security programme	Information security commitment
58. Information security is perceived as important by executives.	Information security leadership	Management buy-in
59. Action (e.g. disciplinary procedure) should be taken against anyone who does not adhere to the information security policy (e.g. if they share passwords, give out confidential information or visit prohibited internet sites).	User management	Information security accountability
60. My division clearly outlines what is expected of me with regard to information security.	Information security leadership	Information security commitment
61. I believe X's employees adhere to the information security policy.	Information security leadership	Information security commitment
62. My division encourages adherence to the information security policy.	Information security leadership	Information security commitment
63. I believe there is a need for additional training to use information security controls in order to protect information.	Training and awareness	Information security accountability
64. I believe the information security awareness initiatives are effective.	Training and awareness	Information security commitment
65. My colleagues take care when talking about confidential information in public places.	Privacy perception	Information usage perception
66. X has clear directives on how to protect sensitive/confidential client information.	Privacy perception	Information security commitment
67. X has clear directives on how to protect sensitive/confidential employee information.	Privacy perception	Information usage perception
68. I believe that it is important to limit the collection and sharing of sensitive, personal information.	Privacy perception	Information usage perception
69. I believe X's client data is complete and accurate.	Privacy perception	Information usage perception
70. My colleagues ensure that client information is protected (e.g. encrypted) when taken off site.	Privacy perception	Information usage perception

ISCA statements	Original ISCA dimensions	New factor name
71. I would feel comfortable if X monitored what I posted on social networking sites.	Privacy perception	Not included
72. It is acceptable to me if employees were disciplined if they posted inappropriate comments about X on social networking sites.	Privacy perception	Not included
73. I believe that access to social networking sites will enhance my work activities.	Privacy perception	Not included

References

Abdulkadhim, H., Bahari, M., Bakri, A. and Ismail, W. (2015), "A research framework of electronic document management systems (EDMS) implementation process in government", *Journal of Theoretical and Applied Information Technology*, Vol. 81 No. 3, pp. 420–432.

AlHogail, A. (2015), "Design and validation of information security culture framework", *Computers in Human Behaviour*, Vol. 49, pp. 567–575.

AlHogail, A. and Mirza, A. (2014), "A framework of information security culture change", *Journal of Theoretical and Applied Information Technology*, Vol. 64 No. 2, pp. 540–549.

Ashenden, D. and Sasse, A. (2013), "CISOs and organisational culture: Their own worst enemy?", *Computers and Security*, Vol. 39 No. 2013, pp. 396–405.

Basu, C. (n.d.), "Pros and cons of the congruence model", available at: http://smallbusiness.chron.com/pros-cons-congruence-model-36161.html (accessed 20 March 2018).

Berry, M.L. and Houston, J.P. (1993), *Psychology at work*, Brown and Benchmark, Wisconsin.

Boje, D.M., Burnes, B. and Hassard, J. (2012), *The Routledge companion to organisational change*, Routledge, Oxon.

Bridges, W. (2003), *Managing transitions: Making the most of change*, Perseus Books Group, Reno.

Bryman, A. (2012), *Social research methods*, 4th ed., Oxford University Press, New York.

Byars, L.L. and Rue, L.W. (1997), *Human resource management*, 5th ed., McGraw-Hill, Boston.

Change Activation. (2018), "Change management model guide", available at: http://changeactivation.com/change-management-models/ (accessed 20 March 2018).

Coghlan, D. and Brydon-Miller, M. (2014), *The SAGE encyclopaedia of action research*, Sage Publications, Los Angeles.

Connolly, L.Y., Lang, M., Gathegi, J. and Tygar, D.J. (2017), "Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study", *Information & Computer Security*, Vol. 25 Issue: 2, pp.118–136.

Cooper, D.R. and Schindler, P.S. (2003), *Business research methods*, 8th ed., McGraw-Hill, USA.

Da Veiga, A. and Eloff, J.H.P. (2010), "A framework and assessment instrument for information security culture", *Computers & Security*, Vol. 29 No. 2010, pp. 196–207.

Da Veiga, A. and Martins, N. (2015a), "Improving the information security culture through monitoring and implementation actions illustrated through a case study", *Computers & Security*, Vol. 49 No 2015, pp.162–176.

Da Veiga, A. and Martins, N. (2015b), "Information security culture and information protection culture: A validated assessment instrument", *Computer Law and Security*, Vol. 31 No 2015, pp. 243–256.

Da Veiga, A. and Martins, N. (2017), "Defining and identifying dominant information security cultures and subcultures", *Computers & Security*, Vol. 70 No. 2017, pp. 72–94.

Detert, J., Schroeder, R. and Mauriel, J.A. (2000), "Framework for linking culture and improvement initiatives in organisations", *The Academy of Management Review*, Vol. 25 No. 4, pp. 850–863.

Dhillon, G. Syed, R. and Pedron, C. (2016), "Interpreting information security culture: An organizational transformation case study", *Computers & Security*, Vol. 56 No. 2016, pp. 63–69.

Ernst & Young. (2015), *Creating trust in the digital world: EY's global information security survey 2015*, available at: http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf (accessed 20 March 2018).

Goldratt, E.M. (1999), *What is this thing called theory of constraints and how should it be implemented?*, North River Press, Great Barrington.

Haydon, L. (2016), *People centric security - Transforming your enterprise security culture*, McGraw-Hill Education, United States of America.

Herold, R. (2011), *Managing an information security and privacy awareness and training program*, Taylor and Francis Group, Boca Raton.

Hiatt, J.M. (2006), *ADKAR: A model for change in business, government and our community, how to implement a successful change in our personal lives and professional careers based on Prosci research*, Prosci Research, Loveland, Colorado.

Howell D.C. (1995), *Fundamental statistics for the behavioural sciences*, third edition, International Thomson Publishing, California.

IBM. (2013) IBM SPSS Statistics Version 22.0. (2013) IBM Software Group, Chicago, IL.

Information Security Forum (ISF). (2002), *ISF information security awareness report*, s. I, Information Security Forum, UK.

Information Security Forum (ISF). (2007), *The standard of good practice for information security* (SOGP), Information Security Forum, UK.

ISACA. (2007), "COBIT 4.1: Framework for IT governance and control", available at: http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx (accessed 20 March 2018).

ISO/IEC. (2013), *ISO/IEC 27002: Information technology – security techniques – code of practice for information security management*, BSI, Kay Westlake.

Jex, S.M. and Britt, T.W. (2008), *Organisational psychology: A scientist-practitioner approach*, 2nd ed., John Wiley and Sons, New Jersey.

Kanter, R.M., Stein, B.A. and Jick, T.D. (1992), *The challenge of organizational change*, The Free Press, New York.

Kazmi, S.A. and Naarananoja, M. (2014), "Collection of change management models – an opportunity to make the best choice from the various organisational transformational techniques", *GSTG International Journal on Business Management (GBR)*, Vol. 3. No. 3, pp. 71–79.

Kiani, A. and Shah, M.H. (2014), "An application of ADKAR change model for the change management competencies of school heads in Pakistan", *Journal of Managerial Sciences*, Vol. VIII No. 1, pp. 77–95.

Kotter, J.P. (2006), "Leading change – why transformation efforts fail", *Harvard Business Review*, January 2007, pp. 1–10.

Kotter, J.P. (1996), *Leading change*, Harvard Business School Press, Boston.

Krejcie, R.V. and Morgan, D.W. (1970), "Determining sample size for research activities", *Educational and Psychological Measurement*, Vol. 30, pp. 607–610.

Lacey, D. (2010), "Understanding and transforming organizational security culture", *Information Management & Computer Security*, Vol. 18 No. 1, pp. 4–13.

Leban, B. and Stone, R. (2008), *Managing organisational change*, 2nd ed., John Wiley & Sons, New York.

Lewin, K. (1947), “Frontiers in group dynamics: Concept, method and reality in social science; social equilibria and social change”, *Human Relations*, Vol. 1 No. 1, available at: http://hum.sagepub.com/content/1/1/5.full.pdf+html (accessed 20 March 2018).

Lewin, K. (1951), *Field theory in social science*, Harper and Row, New York.

Luecke, R. (2003), *Managing change and transition*, Harvard Business School Press, Boston.

Martins, E. and Martins, N. (2016), “Organisational culture”, in Robbins, S.P., Odendaal, A. and Roodt, G. (eds), *Organisational behaviour*, 3rd ed., Pearson Education, Cape Town, pp. 606–641.

Nadler, D. and Tushman, M. (1980), “A model for diagnosing organizational behavior”, *Organizational Dynamics*, Vol. 9 No. 2, pp. 35–51.

National Institute of Standards and Technology (NIST). (2016), *Special publication 800-12: An introduction to computer security: The NIST handbook*, available at: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf (accessed 20 March 2018).

Ngo, L., Zhou, W. and Warren, M. (2005), Understanding transition towards information security culture change, *Proceedings of the 3rd Australian Information Security Management Conference*, Edith Cowan University, 2007, Australia, pp. 67–73.

Ogbonna, E. (1992), “Managing organisational culture – fantasy or reality”, *Human Resource Management Journal*, Vol. 3 No. 2, pp. 42–54.

Okere I., Van Niekerk, J. and Carroll, M. (2012), “Assessing information security culture: A critical analysis of current approaches”, *Information Security South Africa (ISSA)*, July, pp. 1–8.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T. (2017), “The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies”, *Computers & Security*, Vol 66 No 2017, pp. 40–51.

Patrick, F.S. (2001), “Using resistance to change (and the TOC thinking processes) to improve improvements”, *IIE Solutions Conference proceedings*, 2001, Institute of Industrial Engineers, Norcross.

PCI Security Standards Council. (2016), “*PCI DSS requirements and security assessment procedures (Version 3.2)*”, available at: https://www.pcisecuritystandards.org/document_library, (accessed 20 March 2018).

Plunkett, W.R. and Attner, R.F. (1994), *Introduction to management*, 5th ed., Wadsworth Publishing Company, Belmont.

PricewaterhouseCoopers (PwC). (2016), *The global state of information security survey 2016*, available at: https://www.pwc.com/sg/en/publications/global-state-of-information-security-survey.html (accessed 27 March 2018).

PricewaterhouseCoopers (PwC). (2018), *The global state of information security survey 2018*, available at: http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html (accessed 20 March 2018).

Prosci. (2013), *Prosci’s benchmarking study*, available at: https://www.prosci.com/change-management/thought-leadership-library/change-management-methodology-overview (accessed 20 March 2018).

Robbins, S.P., Judge, T.A., Odendaal, A. and Roodt, G. (2016), *Organisational behaviour*, 3rd ed., Pearson, Cape Town.

Rossouw, D. and Van Vuuren, L. (2013), *Business ethics*, 5th ed., Oxford University Press, South Africa.

Ruighaver, A.B., Maynard, S.B. and Chang, S. (2007), “Organisational security culture: Extending the end-user perspective”, *Computers & Security*, Vol. 26 No. 2007, pp. 56–62.

Scantron (2018), SurveyTracker, available at: http://www.scantron.com/software/survey/surveytracker-plus/overview (accessed 27 March 2018).

Schein, E.H. (1985), *Organizational culture and leadership*, Jossey-Bass, San Francisco.

Schein, E.H. (2006), *Cultures and organizations: Software of the mind*, 3rd ed., John-Wiley and Sons, San Francisco.

Schlienger, T. and Teufel, S. (2005), "Tool supported management of information security culture", in Sasaki, R., Qing, S., Okamoto E. and Yoshiura,H. (eds.), *IFIP 20th International Information Security Conference proceedings*, 2005, Springer, Japan, pp. 65–77.

Schlienger, T. and Teufel, S. (2003), "Analyzing information security culture: Increased trust by an appropriate information security culture", *Proceedings of the International Workshop on Trust and Privacy in Digital Business (TrustBus 2003) in conjunction with the 14th International Conference on Database and Expert Systems Applications (DEXA 2003)*, 2003, Prague.

Sheperd, M.L., Harris, M.L, Chung, H. and Himes, E.M. (2014), "Using the Awareness, Desire, Knowledge, Ability, Reinforcement Model to build a shared governance culture", *Journal of Nursing Education and Practice*, Vol. 4 No. 6, pp. 90–104.

Sherif, E., Furnell, S. and Clarke, N. (2015), "An identification of variables influencing the establishment of information security culture", in Tryfonas, T. and Askoxylakis, I. (eds), *The human-computer Interaction (HCI) Conference – human aspects of information security, privacy and trust (HAS)*, 2015, Springer, Los Angeles, pp. 436–448.

Todnem, R. (2005), "Organisational change management: A critical review", *Journal of Change Management*, Vol. 5 No. 4, pp. 369–380.

Tree Solution. (2018), "Sicherheitskultur", available at: http://www.treesolution.ch/10-0-Smart-Tools-fuer-mehr-Sicherheit.html (accessed 20 March 2018).

Van Niekerk, J. and Von Solms, R. (2005), "A holistic framework for the fostering of an information security sub-culture in organizations", in Venter, H.S., Eloff, J.H., Labuschagne, L. and Eloff, M.M. (eds), *The Information Security South Africa Conference (ISSA2005) proceedings*, 2005, ISSA, Johannesburg.

Van Niekerk, J. and Von Solms, R. (2006) "Understanding Information Security Culture: A Conceptual Framework", in Eloff, J.H., Labuschagne, L.,Eloff, M. M. and Venter, H.S. (Eds), *The Information Security South Africa Conference (ISSA2006) proceedings*, 2006, ISSA, Johannesburg.

Verizon. (2017), *Data breach investigations report*, 10th ed., available at: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/ (accessed 20 March 2018).

Whitman, M.E. and Mattord, H.J. (2017), *Management of information security*, 5th ed., Cengage Learning, Australia.