Defining and identifying dominant information security cultures and subcultures

Adéle da Veiga[a] and Nico Martins[b]

[a]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

[b]Department of Industrial and Organisational Psychology, University of South Africa, P.O. Box 392, UNISA 0003, South Africa, martin@unisa.ac.za

Abstract

When considering an information security culture in an organisation, researchers have to consider the possibility of several information security subcultures that could be present in the organisation. This means that different geographical, ethnic or age groups of employees could have different assumptions, values and beliefs about the protection of information, resulting in unique information security subcultures. This research sets out to understand how dominant information security cultures and subcultures develop and how they can be influenced positively over time through targeted interventions.

An empirical case study was conducted using a survey approach with a validated information security culture questionnaire to illustrate how to identify dominant information security cultures and subcultures. The survey was conducted at four intervals in the same organisation over a number of years to identify potential information security subcultures and to monitor the change, if targeted interventions for each are implemented. Using t-tests and ANOVA tests, a number of information security subcultures were identified, mostly evident across the organisation's office locations (which are separated geographically), as well as between employees that worked in the IT division compared to those who did not. The data indicates that the dominant information security culture and subcultures improved over time to a more positive information security culture after the implementation of targeted interventions. This illustrates how the identification and targeting of information security subcultures with customised interventions can influence the information security culture positively. By using information security interventions, organisations can target their high-risk subcultures and monitor the change over time through continuous assessment, thereby minimising the risk to information protection from a human perspective.

Keywords: Information security culture, subculture, dominant culture, influence, assess, change, quantitative research

1. Introduction

An information security (IS) culture is a critical component of an organisation's IS programme. It has to be embedded in the organisation, changed and influenced to direct employee, contractor and third-party behaviour, thereby reducing risk to the organisation's information assets. Depending on how the organisation is structured and who is responsible for the governance of information, the task of instilling or changing an IS culture belongs to senior or executive leadership, who are often part of a governance committee with several roles ranging from compliance, risk, ethics and privacy to information technology. The first questions asked by those responsible would be: What is the dominant IS culture and which IS subcultures are present?, What interventions are required to positively influence the dominant IS culture and subcultures?

There are numerous studies indicating which factors influence IS culture with the objective of transforming the culture [4, 18, 20, 28, 29, 46, 50, 62, 67, 69, 75, 80]. These factors include aspects such as management, awareness, training, policies, compliance and national culture. One factor on which limited research has been conducted is deviations from the dominant IS culture, which are present in IS subcultures. Schlienger and Teufel [66] and Van Niekerk and Von Solms [78] refer to IS subcultures as being part of the overall organisational culture. Their research, however, does not extend to the identification of IS subcultures and how to target and prioritise interventions for identified IS subcultures. Faily and Fléchais [108] found that subculture norms could influence the perception of security and emphasised that a security culture could include various subcultures.

Most organisations have a dominant culture and subcultures. In the context of the dominant culture, the majority of the employees share the organisation's core values, whereas in a subculture, a smaller group of employees share common values related to their work environment, department, geographical area, peer group or nationality [51]. These smaller groups of employees could include contractors, service providers or suppliers who could exhibit work values different from those of the organisation. The sources of security incidents in organisations are attributed not only to employees, but also to third parties, such as service providers, consultants, contractors and suppliers or partners [87, 88]. These third parties should also comply with the organisation's IS and privacy policies [89] and as such are included when referring to employees in the context of dominant IS cultures and subcultures.

Hofstede, Hofstede and Minkov [37] conducted a large study across 70 countries to examine how workplace values have an impact on the organisation's culture and to establish how the organisational culture relates to the national culture of each of the countries. In their study, they found that the national culture of each country differs and they related this to the concept of subcultures. Subcultures have been researched significantly in the industrial psychology research field from a national and organisational culture perspective [37, 49, 51, 59, 64, 65, 90, 91].

One could argue that IS culture is part of the organisational culture [66, 78] and describe it as a construct within the organisational culture. In an ideal world, one would expect all employees to share similar values and resultant behaviour, thereby forming a consistent IS culture across the organisation. However, this is not always the case. At an organisation's head office, where most of the employees might be stationed, employees could share similar values to protect information, for example "all information must be accurate", "all client information must be treated as confidential" or "passwords must never be shared". Employees in a branch located in the country might perceive risks to information differently. They might feel that they can share their passwords to help one another get work done quicker. A subculture emerges in the branch that is different from the dominant IS culture at their head office, generating different threats to the protection of the organisation's information. By implication, one organisation could have a number of IS subcultures across its office locations, gender groups or generation groups, job levels, and so on, each varying from the dominant IS culture [51, 65, 91]. A subculture is thus a group of employees in an organisation that has a subculture differing from the dominant culture [51, 59, 90, 91]. When a culture belonging to a group, such as a certain department, age, gender or job level, varies or deviates from the organisation's dominant culture, it is referred to as a subculture [49, 51, 90, 91].

This has a significant implication when aiming to instil and/or change an IS culture. The same approach cannot be used across the organisation as there may be various subcultures within an organisation requiring different training or awareness needs with regard to IS. Different subcultures could pose varying risks [93] if their values and norms are in conflict with those of the dominant culture [51, 92]. Similarly, the action plans or interventions required to strengthen a positive IS subculture to become a dominant culture or to change a conflicting IS subculture could vary, and management would need to implement unique initiatives to address each [92, 93]. Therefore, management might have to devise different action plans to direct and influence the different IS subcultures to effectively instil an overall strong IS culture across the organisation. However, the prevalence of IS subcultures across an organisation has not been researched before; therefore no empirical data is available as yet.

2. Research objectives

The first objective of the research was to understand the concept and development of dominant IS cultures and subcultures in the context of IS culture. The second objective was to illustrate how to identify IS subcultures and further more to establish if there is an impact on the IS subcultures if focused interventions are implemented. To achieve the research objectives, a survey was conducted in an international organisation to identify if IS subcultures were present, using statistical analysis, and to monitor the change over a period of time.

The remainder of the paper is structured as follows: section 3 gives the background to IS culture. The concepts of dominant IS culture and subcultures are explained and defined in section 4. Section 5 provides an overview of existing literature on factors that could influence the IS culture. Section 6 covers the development of an IS culture incorporating the concepts of dominant culture and subcultures. It is followed by a discussion about the measurement of an IS culture in section 7. Section 8 follows with the empirical case study and an outline of the results. A discussion of the research results and limitations is presented in section 9, followed by the conclusion.

3. Background to information security culture

An IS culture has been defined by various researchers [3, 19, 20, 44, 66]. It relates to the way things are done in the organisation to protect information [20], which is visible in artefacts (e.g. posters on online training), collective values, norms and knowledge (e.g. customer information is valuable and should be protected) and basic assumptions (information is a strategic asset) [64, 65, 66, 80].

An improved IS culture can aid organisations in reducing risk to information in a way that is similar to how the industrial industry improves safety culture to minimise safety risk [41]. The focus on safety culture has been used successfully in the oil and gas, railway and aviation industries [41, 95] where various methods have been implemented to reduce accidents and improve safety performance [41]. One such project relates to the safety culture maturity model (SCMM), which was developed as part of the Keil project [96] with the objective of aiding organisations to progress to the most mature level of safety culture. Its definition of an organisation's safety culture also relates to attitudes, values, beliefs and organisational symbols (i.e. artefacts) to aid organisations to address behavioural and cultural issues of employees in order to improve safety [96].

However, understanding the perception of risk is a challenge as the "perceptions of right and truth depend on cultural categories", as argued by Douglas and Wildavsky [97]. They also emphasise that the perceptions of risk are related to individual personalities where the individual's perception of risk is influenced by their cultural bias, as supported through cultural theory [98, 103]. The cultural theory of risk is concerned with four types of cultural groups, each with their own social norms and cultural bias, which influence the way in which they perceive risk and make decisions [97, 98, 100, 103].

This has the implication that what could be perceived as a risk in one culture or by a certain individual might not be perceived as such by another. From an IS perspective, this has the implication that the perception of risk related to IS could vary among employees. This lends itself to the concept of prevailing subcultures that could exist in an organisation where employees have varying perceptions of IS risk as a result of their cultural bias, personalities, age or other demographic factors [51, 97, 98].

Hofstede's work on culture [37] has been regarded as one of the most widely cited [102]. His work focuses on cross-cultural relationships and he defined five dimensions serving as characteristics that can be measured across nations using a survey method. Although his work has been used in industry and by academics, it is not short of criticism. Many researchers criticise the sampling method used by Hofstede – he concentrated on one organisation and included nations as a group, whereas nations include ethnic units [102]. What is relevant in Hofstede's work to this study is the concept of subcultures which exist across nations in the same manner that they could exist in an organisation [37, 51].

IS culture was studied in this research from an organisational culture perspective where subcultures could be present [51]. Organisational culture, which is "a system of shared meaning" held by employees, can be seen from an integrated perspective, but also as separate groups within the same organisation where "the organisational culture is a blend of subgroup cultures" [51]. Martins and Martins [51] define a dominant culture as "a culture that expresses the core values that are shared by a majority of the organisation's members". They define subcultures as "mini-cultures within an organisation, typically defined by department designation and geographical separation". Pheysey [59] refers to a culture as "a way of seeing what is common to many people". She also affirms that there are often subcultures present in an organisation, which represent "ways of seeing by minorities". Zellmer-Bruhn et al. [85] confirm that a subculture is a "distinctive group within an organisation" whose members interact with one another and often share the same problems or concerns.

4. Information security subcultures

Researchers [66, 78] refer to IS culture as a subculture of the organisational culture. In this instance, the organisational culture represents the dominant culture as “the way things are done and seen by the majority of the employees”. The IS culture falls within the context of the organisational culture directed through leadership, the strategy and organisational policies, but also the IS policy. Within the IS culture, mini-cultures or subcultures are differentiated between groups of employees. The differentiation is based on various groups of employees in an organisation, such as their geographical location, office location, job level, generation group, gender or religion [51, 90, 91]. Various IS subcultures can therefore exist in an organisation which can be in line with the dominant IS culture or oppose it – this is referred to as a counterculture [49].

It cannot be assumed that IS subcultures exist between groups of employees in an organisation, for example across its geographical locations or job levels. To establish if IS subcultures exist, a quantitative survey can be conducted to derive data that can be used through statistical analysis to identify the subcultures. Martins and Van der Ohe [52] applied t-tests and the one-way analysis of variance (ANOVA) to identify significant differences between biographical groups in organisational culture surveys. The significant differences were identified in the overall means between the biographical groups, such as job levels, departments, office locations, age groups and so on. Significant differences were an indication of prevailing subcultures [52]. The t- test and ANOVA tests can therefore be applied in quantitative research to identify subcultures across demographic groups.

Management can change culture by identifying the most effective subcultures in the organisation and using them as an example of model behaviour for other groups [33]. Only once the existing IS culture (dominant IS culture and subcultures) is understood can interventions be implemented to direct IS subcultures to share common views on the protection of information. By measuring and identifying the dominant IS culture and subcultures, management ensures employees that they are paying attention to IS and thus reinforcing the culture [64].

In summary, a dominant IS culture is defined by the researchers as the culture where IS values, perceptions and policy principles are shared by the majority of the organisation’s members. An IS subculture is a distinctive group of employees that share IS values, perceptions and policy principles that deviate from those shared by the majority of the organisation’s members. The term ‘information security culture’ is used by the researchers to describe the combined culture of both the dominant IS culture and subcultures without making a distinction between the IS culture of various demographic groups across the organisation.

5. Factors influencing information security culture

This section provides a summary of factors found in existing research that could potentially influence the IS culture in a planned manner to transform/change it. The aim is to determine if there are existing approaches focusing on dominant IS cultures and subcultures. Various researchers have proposed factors that could potentially influence an IS culture as summarised in Table 1. The factors are listed in column 1 and the researchers who proposed the factors that could influence IS culture are identified in column 2. Column 3 indicates whether the factor is regarded as an intrinsic or extrinsic influence on IS culture. Extrinsic influence refers to factors external to the individual (i.e. employee) that could influence the organisation's IS culture [57]. Intrinsic influence refers to intrinsic factors related to the individual, such as personality, which could influence the way the person perceives IS from their frame of reference, personality or experience [57]. A description of the factors is given in column 4. Although there are various technology and process aspects that play a critical role in IS, only the factors regarded as relevant from a human perspective are included.

Factors influencing IS culture	**Researchers**	**Intrinsic/ extrinsic factor**	**Description**
1. Management	Ngo et al. [54] ISF [41] Van Niekerk and Von Solms [78] Thomson et al. [75] Johnson and Goetz [43] Ruighaver et al. [62] Dojkovski et al. [24] Da Veiga and Eloff [19] Hu et al. [39] Wilderom et al. [82] Sherif et al. [69] AlHogail [3] Flores and Ekstedt [26] Faily and Fléchais [108]	Extrinsic	Management or leadership and their roles in the organisation are critical in forming the desired culture. They need to define the organisation's IS strategy and lead by example.
2. IS policies	ISF [41] Vroom and Von Solms [81] Thomson et al. [75] Knapp et al. [45] Alnatheer and Nelson [5] Da Veiga and Eloff [19] Box and Pottas [11] Da Veiga [18] Sherif et al. [69]	Extrinsic	Employees' knowledge and perception of IS policy rules and procedures could positively influence the IS culture. This policy is a critical cornerstone to direct the IS culture and serve as a foundation to create shared values and beliefs.
3. Workplace capabilities	ISF [41] Furnell and Rajendran [28] Padayachee [57]	Extrinsic	Internal capabilities of the organisation can influence the culture – aspects such as the usability of systems, employee turnover, reliance on temporary employees, the competency of employees and effectiveness of monitoring procedures, job satisfaction, task pressure, task significance, security practices, disciplinary procedure, security monitoring, supervision, performance and reward.

Factors influencing IS culture	Researchers	Intrinsic/ extrinsic factor	Description
4. Risk and response factors	OECD [56] ISF [41] Munteanu and Fotache [53] Shameli-Sendi et al. [68] Sabbagh and Kowalski [100]	Extrinsic	Focusing on an IS risk culture to minimise IS risk. The manner in which organisations identify, prevent, detect and respond to security incidents impacts the IS culture.
5. Operational management	Shameli-Sendi et al. [7] Knapp et al. [45] Hassan and Ismail [31]	Extrinsic	Organisations should have a comprehensive approach to manage and govern IS based on a risk assessment approach. Proper management, review, audit and monitoring will aid in directing a positive IS culture.
6. Training and awareness	Albrechtsen [1] Nosworthy [55] OECD [56] Van Niekerk and Von Solms [78] Thomson et al. [75] Flores and Ekstedt [26] Dojkovski et al. [24] Alnatheer and Nelson [5] Herold [35] Kruger et al. [48] Hassan and Ismail [31] Hovav and D'Arcy [38] Parsons et al. [58] Sherif et al. [69] Da Veiga and Martins [20] AlHogail [3] Safa et al. [105]	Extrinsic	IS awareness and training are implemented to educate employees to understand the risk to information and the relevant controls to use and policies to abide by. Training and awareness have been proven to have a positive impact on the IS culture over time.
7. Change management	Ngo et al. [54] Hassan and Ismail [31] AlHogail [3]	Extrinsic	Change to technology in the organisation helps increase security, quality, efficiency and reliability, which have a significant impact on the functionality, usability, privacy and security of the data. Change management processes should be incorporated in technology changes and aid employees with the integration and acceptance of change for it to become part of the culture.
8. National and organisational culture	Dojkovski et al. [23, 25] Alnatheer and Nelson [5] Alfawaz et al. [2] Flores et al. [27] Sherif et al. [69]	Extrinsic	The society in which the organisation operates impacts on the IS culture – in some societies free flow of information, openness and transparency are upheld and in others, the flow of information is restricted. These national cultural factors impact the way information is processed and protected and ultimately affect the IS culture.
9. Knowledge	Zakaria [84] Van Niekerk and Von Solms [79]	Extrinsic/ Intrinsic	IS knowledge is created through implicit and explicit means to embed security obedience. Individuals have their own knowledge and

Factors influencing IS culture	Researchers	Intrinsic/ extrinsic factor	Description
	Thomson et al. [75] Hassan and Ismail [31]		understanding of information security, which influences how they process information and use information security controls.
10. Security behaviour	Vroom and Von Solms [81] Ngo et al. [54] Albrechtsen [1] Herath and Rau [34] Alfawaz et al. [2] Da Veiga and Eloff [19] Gabriel and Furnell [29] Hassan and Ismail [31] Sherif et al. [69]	Intrinsic	Implementing security components impacts on the interaction of employees with information assets, and employees consequently exhibit certain behaviour referred to as security behaviour. The objective is to instil security behaviour conducive to the protection of information assets based on the organisation's policies.
11. Security compliance	Furnell and Thompson [29] Tsohou et al. [76] Parsons et al. [58] Sherif et al. [69]	Intrinsic	The workforce's knowledge of the IS policy and procedures will have a positive impact on their attitude towards the IS policies and on compliance. In an organisation where there is a strong or healthy IS culture, one would expect compliance as a visible trait of the culture.
12. Soft issues – workplace independent	Furnell and Thomson [29] Gabriel and Furnell [30] Hu et al. [39] Parsons et al. [58] Furnell and Rajendran [28] Padayachee [57] Sherif et al. [69] Faily and Fléchais [108]	Intrinsic	Soft issues relating to the employees could also impact on the IS culture, such as real-life exposure, security-related incidents, media coverage, personal benefits, group/community benefits and awareness, acceptance of policy, competence, etiquette, commitment, obedience, self-disapproval and ethics. Subculture norms can also influence the information security culture.

Table 1: Summary of factors influencing IS culture

What is important is that none of the factors distinguish between the dominant IS culture or subculture, apart from the work of Schlienger and Teufel [66] and Van Niekerk and Von Solms [78] who refer to the IS culture as a subculture of the overall organisational culture. Their work does not extend to explore the concept of dominant IS cultures and IS subcultures and how to identify or implement targeted interventions for the various IS subcultures. Faily and Fléchais [108] have developed a model in which subcultures should be considered as part of the IS culture. They identified a subculture based on the participants' different perceptions of security, for example in handling data and descriptions of controls. Their approach does however not extend to a method whereby the holistic information security culture is determined and variations thereof in the sense of subcultures are identified across a large international organisation. While these researchers used a qualitative method, it could be a challenge for a large international organisation to repeat similar interviews to identify potential subcultures.

6. Development of an information security culture

The development of an organisational culture can be referred to in order to ascertain how an IS culture develops. An organisational culture develops where executives and management develop a vision and strategy for the organisation. The vision and strategy are often depicted in organisational policies and procedures. Employee behaviour will become evident as guided by the vision, strategy and policies. Over time an organisational culture emerges that encapsulates the vision and strategy as well as the experiences employees had when implementing them [33]. An IS culture component (or construct) develops in an organisation in the same way as the organisational culture. The development of an IS culture, as depicted in Figure 1, is adapted from the work of Hellriegel [33]. Figure 1 includes the concepts of dominant IS culture and subcultures to illustrate their development in the organisation.

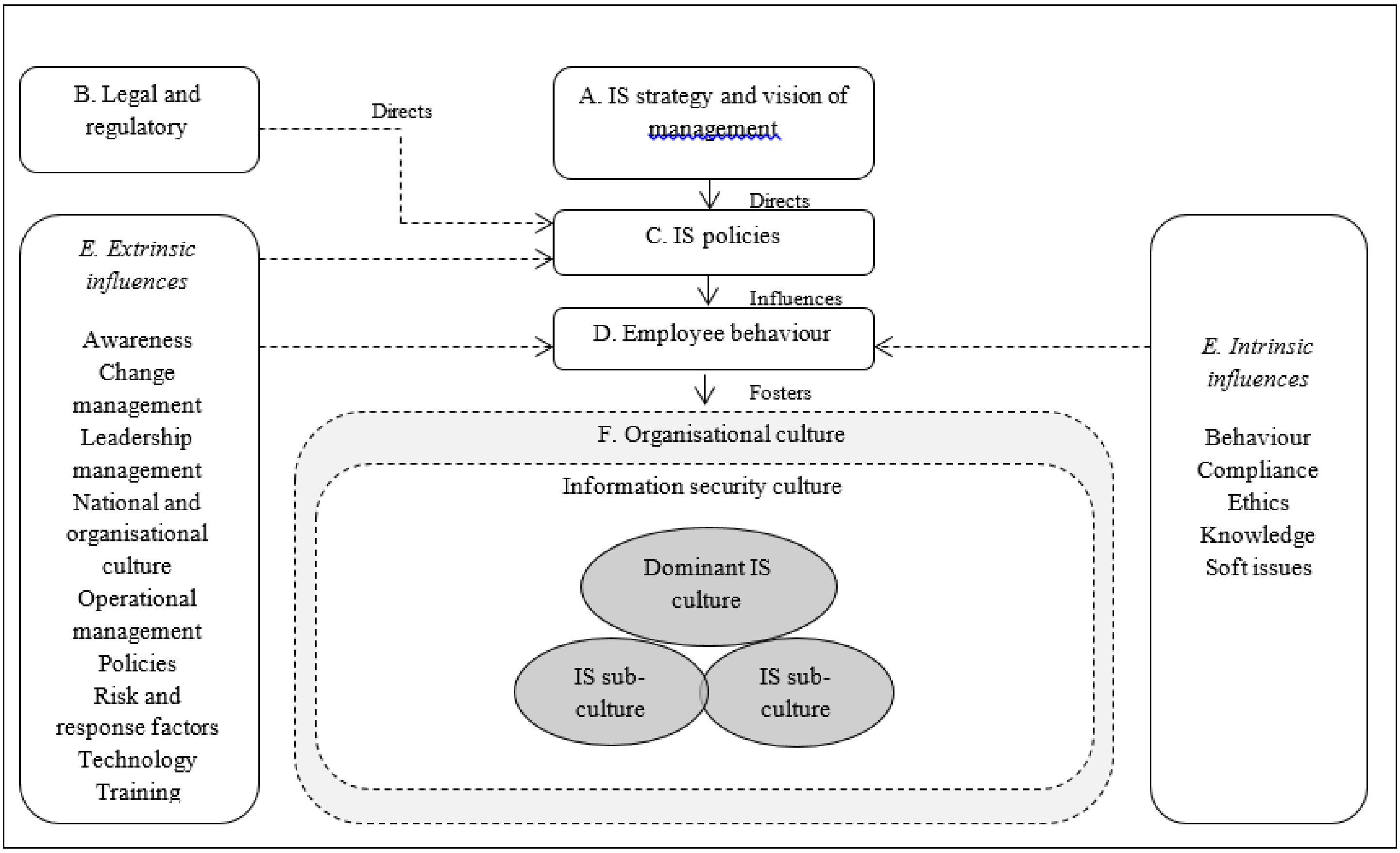


Fig. 1: Development of an IS culture adapted from Hellriegel [33] to include subcultures and intrinsic and extrinsic influences

6.1 A. Information security strategy and vision of management

Management is regarded as the main “shaper and builder” of culture in an organisation [39]. Schein [64] summarises the function of leadership as the “creation and management of culture”. Management therefore outlines the vision and strategy of the organisation [33]. The King III report from the Institute of Directors of Southern Africa (IoDSA) [42] states that the board is responsible for ensuring that information assets are managed effectively and should approve the organisation’s IS strategy. The board should delegate responsibility for implementing IS and management needs to demonstrate their commitment and buy-in. This is supported by the UK Corporate Governance Code [77], stating that the directors “should confirm that they have carried out a robust assessment of the principal risks facing the company – including those that would threaten its business model, future performance, solvency or liquidity”. In order to manage information assets effectively, robust risk assessments must be conducted to identify risks, which could relate to the data of customers or data derived from financial statements, the systems and databases supporting the data, as well as the employees who have access to it. This relates directly to the requirements of the Sarbanes–Oxley (SOX) Act of 2002 [71], a United States (US) federal law. SOX [71] outlines the responsibilities of a public corporation’s board of directors, which extend to governance, including risk assessments of internal controls over information systems related to the financial statements.

Van Niekerk and Von Solms [80] refer to the elasticity of an IS culture and management’s role in influencing the values of employees in an effort to gain equilibrium between management’s and employees’ expectations for the protection of information. Ultimately, the leaders of an organisation can influence the culture of the organisation using various approaches to create an environment where information is protected [70]. Ashenden [6] confirms this by stating, “Successful management of information security depends on authority, leadership, vision and good management practice”.

Leadership and senior management play a critical role in influencing or changing the IS culture [75]. Their vision is expressed through means such as the IS policy [75], which provides the direction and intent for the protection of information. They could state in the policy that information is regarded as a valuable business asset whose integrity, confidentiality and availability must be maintained throughout the information life cycle – the policy will govern employee behaviour. In turn, extrinsic and intrinsic factors influence the manner in which employees will respond to the IS policy. The IS culture that emerges could either be conducive to the protection of information or hamper it. It is therefore crucial to assess the IS culture that has emerged and to determine whether it is in line with the initial IS strategy and vision of management.

In summary, Schein [64] emphasises that one of the most powerful techniques to instil and reinforce a culture is to take into account “what leaders pay attention to, measure and control”. Leaders who “externalise their own assumptions, embed them gradually and consistently in the mission, goals, structures, and working procedures of the group” create culture. A culture therefore begins with its leaders – management plays a major role in the institutionalisation of culture [51]. Similarly, an IS culture is instilled by management through their information protection norms and values that filter down to all levels of employees.

6.2 B. Legal and regulatory requirements

One of the board’s responsibilities is to ensure that the organisation complies with applicable laws and regulations [42, 77]. Laws set out to establish “what is right in human interaction and society” [61]. There are several laws that govern information security and privacy. The European Union has comprehensive laws that govern the collection, use and dissemination of personal information in the public and private sector. In Europe, the General Data Protection Regulation (GDPR), which was proposed by the European Commission in 2012 and generally agreed upon by the European Parliament and Council in December 2015 [32], replaced the Data Protection Directive 95/46 [22]. The US follows a sectorial approach in which laws address the protection of personal information in a particular industry. A co-regulatory model is followed in Canada and Australia where the industry develops enforceable standards which are overseen by, for instance, an information and privacy commissioner. Other countries, such as Japan and Singapore, follow a self-regulatory model [74]. In South Africa the Protection of Personal Information Act (PoPI) of 2013 [60] was promulgated in 2013. PoPI [60] includes specific provisions for IS to preserve the integrity, confidentiality and availability of personal information processed by the organisation and any related third parties.

One of the ISO27002 [86] standard’s objectives is compliance with law, statutory, regulatory and contractual obligations for IS, which are regarded as external compliance requirements to be met by the organisation. Another objective of the standard is compliance with IS policies, standards and technical requirements, which are internal compliance requirements to be met by the organisation. Both the internal and external compliance requirements should be implemented in organisations and audited [42, 86]. Researchers have focused on legal and regulatory requirements as an external influence on the development of IS policies [15, 40, 45]. Society and regulations are incorporated in the Information Security Culture Framework (ISCF) of AlHogail and Mirza [4]. They argue that external factors, such as legal and regulatory systems, as well as internal factors, such as the IS policy, are critical components of an IS culture related to compliance requirements.

It is necessary to guide employee behaviour and implement processes and technology safeguards when processing information to be in line with the regulatory requirements. Legal and regulatory requirements also place an obligation on an organisation to ensure that employees are aware of the IS and information privacy requirements. For example, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 [36] of the US requires the implementation of a security awareness and training programme that includes security reminders. Privacy laws require organisations to take accountability for information and for when the information is breached.

Based on the legal and regulatory requirements as well as organisational IS policy requirements, it is imperative that the IS culture facilitates the protection of information and that employees know what can and cannot be done with information. They need to know what they can use information for, who they can share it with and how to protect it throughout the information life cycle. Legal and regulatory requirements have an impact on the manner in which information is processed and ultimately serve as input to IS policies [86]. As such, the IS culture is also influenced by legal and regulatory requirements as an external compliance factor [3, 4]. Internal compliance factors in the organisation should also be considered to direct employee behaviour, such as compliance with the organisation's code of conduct, policies and procedures for internal control over operational and financial controls, IS policies and procedures and contractual requirements [42, 77].

In the absence of an IS policy, there will be no guidelines to protect information from risk such as unauthorised disclosure, access, use or modification, data loss or destruction, incompleteness or inaccuracy [86], which are typically required by privacy laws [22, 32, 60]. Both internal and external compliance requirements must be in line with regulatory requirements and should be embedded in the IS policy [86, 94] to aid in directing employee behaviour and instilling a positive or stronger IS culture [3, 4].

One could expect the IS culture of organisations in different legal jurisdictions to be different, which supports the work of Hofstede et al. [37] in that the values of national culture vary between countries. This could result in different subcultures across data protection jurisdictions for multinational organisations with office locations across different countries. The development of an IS culture is therefore directed by the strategy and vision of management in line with legal and regulatory requirements in different jurisdictions to regulate the IS policy as indicated in Figure 1.

6.3 C. Information security policies and procedures

The IS policy sets out the organisation's approach to IS and provides a framework for setting control objectives and controls, including the structure of risk assessment and risk management [86, 94]. An IS policy is regarded as best practice by ISO27002 [86]. According to the standard, it serves to provide management with "direction and support for information security in accordance with business requirements and relevant laws and regulations". It pertinently incorporates laws and regulations as one of the IS controls, which include laws and regulations relating to IS and data privacy. The IS policy serves as a significant factor to manage and influence the IS culture

[11, 18, 69].

6.4 D. Employee behaviour

Organisational behaviour plays an important role in the development of an organisational culture, as illustrated in Figure 1 and the above description. Through the culture it is clear what behaviour is accepted and encouraged and what not. This can be traced back to management's vision and strategies.

To establish the desired culture in an organisation, it is then necessary to take a look at the organisational behaviour of the employees. The type of culture in an organisation can have a direct impact on the behaviour and actions of the organisation's employees [51]. In an organisation with a bureaucratic culture, where everyone plays by the rules, employees might follow the IS policy more strictly than in a less formal and individualistic culture [83].

Changing an organisation's culture will, in effect, require the focus to be on changing ineffective behaviour and procedures [33]. Subcultures also have an effect on employee behaviour and as such need to be considered by management [92].

6.5 E. Intrinsic and extrinsic influences

The various intrinsic and extrinsic factors relating to the employee, as summarised in Table 1, could influence the IS culture [57]. The intrinsic (i.e. security behaviour, compliance and soft issues) [1, 2, 19, 29, 34, 39, 58, 76] and extrinsic factors (i.e. management, policies, workplace capabilities) [5, 23, 31, 41, 45, 55, 57, 68, 79, 84] play a role in fostering the IS culture, which is evident in the dominant IS culture and subcultures. These factors should be considered in the programme to address IS from a holistic perspective by incorporating the factors that could influence the human element and not only process or technology.

6.6. F. Organisational culture: Dominant IS culture and subcultures

Over time employee behaviour fosters a culture. Certain IS values or perceptions might be common or shared in the dominant IS culture and across the IS subcultures. However, some IS values or perceptions of certain groups of employees could deviate from the dominant culture and can be regarded as IS subcultures.

7. Measurement of information security culture

7.1 Quantitative survey method

It is not easy to measure organisational culture as "culture does not reveal itself easily" [64]. There are various perspectives about the most effective manner in which to measure organisational culture [99]. Schein [64] motivates that a triangulation approach should be used in which various methods are followed to confirm the information obtained in an effort to measure the organisational culture.

Ashkanasy et al. [99] did a study of organisational culture instruments and concluded that quantitative as well as qualitative methods should be used, which supports Schein's view. However, using mixed or multiple methods will increase the cost and time to measure organisational culture. Questionnaires and surveys are an acceptable research method used in the context of social sciences [12] to measure attitudes and opinions of employees [9]. Surveys are found to be effective in measuring the employees' perception about reality rather than reality itself [99]. This extends to focus on what the organisation has as opposed to what the organisation is [101]. The focus as such is on behaviour and attitudes, which can be measured through the perceptions of employees [99]. This aspect makes survey methods useful in measuring organisational culture supported by other advantages such as the collection of large data sets, longitudinal studies, cross-sectional comparisons, benchmarking and change management initiatives, thus increasing the acceptance of the results by employees [14, 107]. An advantage of using a survey method with a questionnaire is that employees can complete it when it is convenient for them to do so and it is an inexpensive manner to obtain data, especially in large organisations where offices are located across countries [107]. The survey method is non-intrusive, especially if it is anonymous [107]. In addition, comparative survey designs allow the researcher to compare two or more independent groups suc h as males with females or various generation groups [106]. Quantitative data also allows the use of statistical analysis to conduct t-tests and ANOVA tests to identify subcultures, following the approach used by Martins and Van der Ohe [52].

Survey methods with a questionnaire have been used with great success in organisational culture studies [99, 110, 111]. According to Ashkanasy et al. [99], questionnaires play an important role in the quantitative analysis of culture because multiple methods are often complex, expensive and time consuming. A limitation of this method is that it might not be effective in measuring the deeper cultural aspects of an organisation [64, 99].

A number of IS culture researchers used a survey, interview or case study method to measure IS culture [44]. AlHogail [3], Schlienger and Teufel [66] and Da Veiga and Martins [20] used a quantitative survey method with a validated instrument to ensure that it is reliable and valid to measure IS culture. Other researchers also used a quantitative survey approach to conduct IS culture studies [6, 26, 44, 67]. In the context of measuring IS culture, the survey method allows the researcher to obtain information about the attitudes and perceptions of employees towards IS in order to identify where change is required to improve the IS culture. The survey method was used as the research method to diagnose the IS culture in this study as a large population was included across countries and the statistical analysis allowed for the use of ANOVA tests to identify the subcultures.

7.2 A process to measure information security culture

The organisational diagnosis (OD) process is used in industrial psychology to measure how an organisation is functioning or performing in order to design change interventions [104]. The OD process is used worldwide [104] and is therefore a popular method that can also be applied to IS culture. OD comprises four key cyclical phases: diagnosing the organisation, planning interventions for improvement, mobilising resources to put the plan into action and evaluating the effects [8, 9, 16, 17, 104]. Byars and Rue [16] state that OD specifically concentrates on the human side of the organisation to change attitudes, values, organisational structures and managerial practices. The following four key phases of OD are adapted to assess an IS culture using quantitative methods:

- *Phase 1: Diagnosing the organisation*

  Management, recognising that the organisation's performance should be improved, can initiate the diagnosing process. In the context of IS, management would recognise that the IS culture should be improved to meet legal, regulatory, contractual, customer, business and policy requirements while minimising risk from a people, process and technology perspective.

In OD, quantitative or qualitative techniques or a combination of them can be used to diagnose the organisation [104]. As part of quantitative techniques, the survey method using a questionnaire can be used to collect data to describe behavioural aspects relating to attitudes and opinions of a representative sample at a point in time [8, 9, 104]. A survey is often conducted within the context of organisational development in which change is instituted afterwards to improve organisational effectiveness [13, 17].

Where an electronic survey method is used in an organisational context, it must be ensured that the sample has access to the Internet or intranet of the organisation in order to access the survey. Alternatively, paper-based surveys can be used, although these increase the cost. One of the benefits of longitudinal studies and comparative analysis is that they can be conducted across a large population and statistical analysis can be used to identify subcultures.

Validity and reliability of the diagnostic instrument (questionnaire)

It is imperative to ensure the reliability and validity of the questionnaire used in survey methods. The concept of validity implies that care must be taken to ensure that the questionnaire assesses what it claims to assess [107, 9, 21]. A valid questionnaire consistently yields reliable and stable results over time [21]. Reliability can be achieved without validity [109]. In other words, although results of a measurement can be reproduced and be consistent, the questions that are asked may be about irrelevant factors. The opposite is true for validity, where a measurement that is unreliable can never be valid. Validity is measured through the use of factor analysis and item analysis. The Information Security Culture Assessment (ISCA) [20] questionnaire used to diagnose IS culture in organisations has been validated and adapted for industry purposes, and has a reliability score of between 0.764 and 0.877 [20].

Identifying the dominant culture and subcultures

The survey data was analysed in terms of means and frequencies. The overall mean of the data of all the statements in the questionnaire is regarded as the score for the dominant culture. “All factors are scored such that a low score indicates non-acceptance of the IS culture dimension while a high score indicates acceptance of the cultural dimension”, according to Martins and Von der Ohe [52]. Management cannot assume that subcultures exist in the organisation. This must first be established. The ANOVA tests (used with more than two groups) or t-tests (used for two groups) can be used to determine if there is a subculture relating to, for example, job levels or age groups. The ANOVA test can indicate which job level/s scored significantly lower or higher compared with the other job levels. For example, the Anova test could indicate that operational employees scored significantly lower (on the overall mean) than middle management. The operational staff where the ANOVA test indicates the significant difference is therefore identified as a subculture for which interventions can be identified. The middle management job level that scores significantly higher is also regarded as a subculture. The other job levels where there are no significant differences are not deemed to be subcultures. This means that the overall means of the other job levels are not significantly different from each other.

Management cannot establish if subcultures exist using a quantitative method if biographical questions relating to specific groups were not included in the questionnaire. It is therefore important to identify the correct biographical questions to include in the questionnaire for employees to answer those questions in the data-gathering phase.

- *Phase 2: Planning interventions for improvement*

  Dominant IS culture and IS subcultures are identified in the diagnosis phases. Management can identify specific areas of improvement for biographical groups that scored significantly lower as indicated

  through the ANOVA or t-test. The data of, for instance, the operational employees can be analysed to identify the lowest scored statements, which would require interventions. This ensures that interventions or customised action plans are targeted at groups where improvement is required and that the improvement plans focus on the correct aspects as identified in the ISCA.

  Certain constructs or statements might also score low on the overall data, reflective of the dominant culture, for which tailored interventions can be developed targeting all the groups of employees.

- *Phase 3: Mobilising resources to put the plan into action*

  A process is formulated to mobilise resources to implement the action plans for the identified subcultures. The interventions could be unique to each subculture as they will be based on the statements or constructs of the group that scored the lowest. Interventions for the dominant culture might also be required if there were statements or constructs that scored low on the overall mean. The interventions could relate to training for certain employee groups or awareness and communication messages tailored to the subculture and to the dominant culture.

  As part of mobilising the resources, various options can be used such as service providers, consultants, internal teams or internal specialists of the origination. A project plan is created to develop and deploy the interventions within the agreed scope and budget approved by management. The implementation of the action plans could span over a few months or even years.

- *Phase 4: Evaluating the effects*

  The change is evaluated by repeating the diagnosis phase and comparing the results to the previous survey's results to identify any improvement and to establish the effectiveness of the interventions for the dominant IS culture and subcultures. Comparative analysis is conducted of the data collected for each of the survey intervals. Through this approach, the IS culture is consistently monitored and directed through interventions.

8. Research methodology

A case study methodology was applied using quantitative methods, including statistical analysis [63] to illustrate how to identify potential IS subcultures. In the context of a case study, a single social unit is studied in depth with intensive analysis in the context of the research problem being investigated [10]. Case studies can be extended to include more than one case in order to conduct comparative analysis. The objective of this research was to understand if there are subcultures in a single organisation, and the organisation is seen as the social unit being studied. This case study can be categorised as a revelatory case study in that a concept that has not been researched before was studied through a case study, namely the identification of IS subcultures and the influence

of focused corrective actions over time. It can also be classified as an intrinsic case study allowing the researcher to better understand the context of the particular case at hand, being the dominant IS culture and IS subculture in a particular organisation [10].

The following section outlines the application of the OD phases in order to identify the dominant IS culture and subcultures.

8.1 Phase 1: Diagnosing the organisation

8.1.1 Measuring instrument

The ISCA questionnaire [20] is used as the diagnostic instrument to assess the IS culture of the organisation. It comprises nine dimensions based on the research model of Da Veiga and Eloff [19]. The questionnaire comprises three sections, namely IS awareness, IS culture and biographical. A total of eighteen IS awareness questions are included in the questionnaire. Table 2 provides an extract of the first ten out of fourteen awareness questions using a yes-no scale. Four questions used a multiple-response scale with a list of options for users to select, such as, "How do you prefer to receive information security messages?".

IS awareness questions extract
1. I know what information security is.
2. I am aware that the organisation has a written information security policy.
3. I have read the information security policy.
4. I know where to get a copy of the information security policy.
5. I know who the group information security officer is.
6. I know who my business unit security officer is.
7. I know what my responsibilities are regarding information security.
8. I know what an information security incident is.
9. I know of an information security breach within my business area within the last 12 months.
10. I have been informed of information security requirements in the last six months e.g. regulations regarding the downloading of email.

Table 2: IS awareness questions extract

Section 2 of the questionnaire includes the IS culture questions, which are based on ten constructs of IS culture [20]:

1. IS management: focusing on user's perception of the protection of assets
2. IS management: focusing on management's perception towards IS management in their division and organisation
3. Change: assessing how the user perceives change management and their willingness to change
4. User management: user awareness and training of requirement to protect information assets
5. IS policies: includes questions regarding IS policy implementation and communication

6. Trust: focuses on trust of employees in the organisation
7. IS leadership: focusing on the governance of IS from a management perspective
8. Training and awareness: assessing the need for training and further awareness
9. Privacy: considering perceptions regarding the protection of employee and customer information
10. IS program management: gauging the perception about the utilisation of IS resources

The IS culture statements are answered using a five-point Likert scale (strongly disagree, disagree, unsure, agree, strongly agree) to assess the employees' degree of agreement or disagreement with the IS culture statements [21]. Table 3 outlines an extract of one statement per dimension.

Dimension	**Statement**
Information asset management	It is important to understand the threats (e.g. theft of equipment, alterations or misuse of information) to the information assets in my division
Information security management	I believe it is necessary for the organisation to monitor compliance with the information security policy
Change	I accept that some inconveniences (e.g. changing my password regularly, locking away confidential documents or making back-ups) are necessary to secure important information
User management	I am aware of the information security aspects relating to my job function
Information security policies	The contents of the Information Security Policy are easy to understand
Trust	I believe that the organisation keeps my private information confidential
Information security leadership	Information security is perceived as important by managers
Training and awareness	I believe the information security awareness initiatives are effective
Privacy	The organisation has clear directives on how to protect sensitive client information
Information security program	I believe it is necessary to commit people to information security

Table 3: IS culture dimensions and question extract

Section 3 of the questionnaire includes biographical questions that are used to identify the number of responses from the various business units, job levels and countries. The biographical questions are used to segment the data, make comparisons between the various groups of employees in the organisation and identify significant differences between groups, which could indicate the existence of IS subcultures.

8.1.2 Organisation

The organisation used in this research is a global bank that operated across twelve countries at the time of the last survey. Its operations relate to a range of specialised financial products and services provided to private clients and organisations. As it operates in the financial sector, it has regulatory and industry requirements for the processing and security of data. The organisation has an established IS programme, IS office function and related policies in place. The Group Information Security Officer (GISO) manages IS from the head office in London with the support of IS coordinators in each country.

All employees employed in this particular organisation were requested to participate and complete the questionnaire. This included all twenty-two offices of the organisation which are all geographically separated across the twelve countries, all job levels and all divisions in the organisation. A web-based survey was sent to all the employees requesting them to answer it anonymously. To motivate employees to participate, they were given the option to enter their e-mail address to stand a chance to win a number of iPads. Their e-mail addresses were not linked with the employee responses in the data file in order to protect their confidentiality and privacy.

The survey was conducted over an extended period (eight years) in 2006, 2007, 2010 and 2013. The same financial organisation, including all its offices, job levels and business units, were surveyed during the four intervals. The data was collected on more than one occasion, but at a single point in time across the dimensions of the same questionnaire. A four- to five-week period was given to employees to respond.

As employees in the organisation participated in the survey voluntarily, it was critical to ensure that enough responses were obtained to conduct the data analysis. As such, the method of Krejcie and Morgan [47] was applied. Table 4 gives a summary of the responses for each of the surveys. The first row portrays the total number of employees employed at that time. Row two indicates the responses required on a 95% confidence level [47]. Row three indicates the actual number of responses obtained for each survey. In all four surveys, an adequate number of responses were obtained according to the 95% confidence level as indicated in the last row.

Survey responses	**2006**	**2007**	**2010**	**2013**
All employee numbers to whom survey was sent	+/- 4 900	+/- 5 300	+/- 7 000	+/- 8 200
Responses required on a 95% confidence level	351	351	364	367
Responses obtained	1 941 (40% response rate)	1 571 (30% response rate)	2 320 (33% response rate)	2 159 (26% response rate)
Adequate number of responses for 95% confidence level	Yes	Yes	Yes	Yes

Table 4: Survey responses

8.1.3 Statistical analysis

Survey Tracker [73] was used to design the electronic questionnaire with the response scales. This software was also used to distribute the questionnaire and collect the data from the employees of the case study organisation. The data was imported to SPSS [72] for the purposes of statistical analysis, such as the ANOVA tests.

8.1.4 Dominant information security culture results

The overall IS culture is represented by the overall mean score for all of the IS culture statements in ISCA, as a representation of the perception of the overall organisation, thus including all biographical areas. Without segmenting the data, the statements that scored the lowest in the IS awareness section as well as the IS culture statements that scored below 4 for the mean [20] were identified. For each of the developmental statements, an intervention was identified (plan interventions phase). Refer to section 8.2 for an extract of the interventions. These interventions were implemented by the organisation's management (mobilise resources phase). The effects were evaluated in the follow-up ISCA that was conducted (evaluate phase).

Table 5 shows the mean and percentage agreement for the IS culture section for each ISCA survey. The results indicate that the IS culture improved over time, with the most positive results in 2013. In 2010 a decline in the results was observed, which could be attributed to the business restructuring that occurred during that period. However, the results in 2013 improved to above 4 for the mean.

ISCA occasion	Frequency	Mean	% agreement
ISCA 4 – 2013	2150	4.10	83.6
ISCA 3 – 2010	1920	3.76	75.7
ISCA 2 – 2007	1563	4.00	81.7
ISCA 1 – 2006	1941	3.89	75.7

Table 5: Overall IS culture section means and % agreement for the four surveys

8.1.5 Information security subculture results

Table 6 gives an overview of the biographical groups and portrays where IS subcultures are identified. The respective job levels, employees who work in IT or not and the office locations (location A to V) are listed in the "Biographical groups" column. The data was segmented to present the number of respondents (frequency) and the overall mean for the IS culture statements for each biographical group for the 2006, 2007, 2010 and 2013 survey. If any of the biographical groups had fewer than five responses, as listed in the frequency column, it was not included in the analysis and "N/A" is listed in the mean columns.

T-tests (two categories) and ANOVA tests (more than two categories) were used to determine if there were significant differences between the biographical groups, for example between all the office locations, for each of the surveys. A significant difference indicates an IS subculture for a specific year [52]. Significant differences between the groups are indicated, with ** being significantly more positive than *. These cells are coloured for ease of reference. Where no significant difference was found between demographic groups, no IS subculture was detected.

There were some respondents in each of the surveys that did not want to disclose their office location and selected the "Other" option. Those employee numbers are listed in the "Other" row. Some respondents did not answer the biographical questions and are indicated in the "No response" row. The total number of responses (frequency) for each of the surveys is depicted in the "Total" row.

Biographical groups	Frequency 2006	Mean 2006	Frequency 2007	Mean 2007	Frequency 2010	Mean 2010	Frequency 2013	Mean 2013
Job level								
Executive	**65**	**3.94**	**71**	**3.97**	**55**	**3.73**	**51**	**4.06**
Manager	**381**	**3.90**	**325**	**4.00**	**419**	**3.79**	**447**	**4.09**
Non-manager	**1470**	**3.89**	**1142**	**4.01**	**1446**	**3.75**	**1645**	**4.10**
Worked in IT								
Worked in IT	**203**	**3.99****	**224**	**4.00**	**338**	**3.79**	**317**	**4.15****
Did not work in IT	**1709**	**3.88***	**1334**	**4.00**	**1582**	**3.75**	**1827**	**4.09***
Office locations								
1. Office A: Australia – Sydney	**77**	**3.97**	**148**	**3.90***	**178**	**3.89***	**167**	**4.04***
2. Office B: Botswana – Gaborone	**3**	**N/A**	**0**	**N/A**	**2**	**N/A**	**1**	**N/A**
3. Office C: Channel Islands – Guernsey	**103**	**4.14****	**67**	**4.13****	**58**	**4.11****	**39**	**4.34****
4. Office D: Channel Islands – Jersey	**60**	**3.95**	**27**	**4.06**	**40**	**4.10**	**14**	**4.22**
5. Office E: Hong Kong – Kowloon	**8**	**N/A**	**0**	**N/A**	**5**	**N/A**	**3**	**N/A**
6. Office F: Ireland – Dublin	**2**	**N/A**	**40**	**4.08**	**51**	**4.14****	**57**	**4.17****
7. Office G: Mauritius – Port Louis	**18**	**4.03**	**31**	**3.97**	**18**	**4.02**	**13**	**4.49****
8. Office H: Namibia – Windhoek	**4**	**N/A**	**1**	**N/A**	**2**	**N/A**	**2**	**N/A**
9. Office I: South Africa – Johannesburg	**848**	**3.85***	**550**	**3.90***	**650**	**3.91***	**587**	**4.07***
10. Office J: South Africa – Cape Town	**232**	**3.85***	**161**	**3.91***	**159**	**3.94**	**162**	**4.10**

Biographical groups	Frequency 2006	Mean 2006	Frequency 2007	Mean 2007	Frequency 2010	Mean 2010	Frequency 2013	Mean 2013
11. Office K: South Africa – Durban and Pietermaritzburg	112	3.88**	85	3.98	77	4.06	29	4.22**
12. Office L: South Africa – Pretoria	83	3.88**	51	3.88*	55	3.99	59	4.13
13. Office M: South Africa – Port Elizabeth	26	3.97	20	4.04	21	3.92	25	4.16
14. Office N: South Africa – East London and Knysna	6	N/A	1	N/A	5	N/A	4	N/A
15. Office O: Switzerland – Geneva	22	3.99	12	4.28**	17	4.16	0	N/A
16. Office P: Switzerland – Zurich	6	N/A	14	4.32**	18	3.92	15	4.35**
17. Office Q: United Kingdom – Abingdon	0	N/A	8	N/A	30	3.86	0	N/A
18. Office R: United Kingdom – London	298	3.92*	340	4.02	621	4.05**	600	4.05*
19. Office S: United Kingdom – Manchester	9	3.81	8	4.12	17	4.12	10	4.20**
20. Office T: United Kingdom – Reading	8	N/A	8	N/A	30	N/A	63	4.18**
21. Office U: United Kingdom – Other	0	N/A	0	N/A	0	N/A	295	4.14

Biographical groups	**Frequency 2006**	**Mean 2006**	**Frequency 2007**	**Mean 2007**	**Frequency 2010**	**Mean 2010**	**Frequency 2013**	**Mean 2013**
22. Office V: United States – New York	**6**	**N/A**	**2**	**N/A**	**5**	**N/A**	**1**	**N/A**
Other	**0**	**N/A**	**4**	**N/A**	**32**	**N/A**	**11**	**N/A**
No response	**10**	**N/A**	**1**	**N/A**	**259**	**N/A**	**2**	**N/A**
Total	**1941**	**N/A**	**1571**	**N/A**	**2320**	**N/A**	**2159**	**N/A**

Table 6: IS subcultures (coloured) indicated on the mean score for the 2006, 2007, 2010 and 2013 surveys (** indicates significantly more positive than *)

The key observations from Table 6 are as follows:

- **Job level biographical groups:** The ANOVA tests indicate that there were no significant differences between the job levels for all four surveys conducted. This implies that there was no significant difference in employee perceptions of the protection of information when comparing the job levels. To further analyse the job levels, the executive management and management employees were grouped (500 employees) and compared with the non-management employees (1 652 employees) using the 2013 data. The means were closely aligned, with 4.08 for management and 4.10 for non-management. At an individual statement level, 13 statements were identified with significant differences, with 8 statements being in favour of non-management. For example, significantly more non-management employees (4.16) believed that the information they worked with was protected adequately compared with management (4.03), as indicated through the t-test. This could indicate that additional or revised controls are required for non-management to protect information. This statement's data can be segmented further at business unit level and country level to identify where the concerns are and what action plans need to be developed.

  It is generally recognised that management plays a significant role in influencing an organisational culture [43]. Similarly, management influences the development of an IS culture [50]. This supports the argument that management plays a significant role in directing and driving an IS culture. The IS norms established by the leaders of the organisation, successfully filtered down to lower job levels, emphasise the importance of strong leaders in developing a strong IS culture. Therefore, one would expect the IS culture of management to direct the culture of non-management employees. If this argument is true, in an organisation where management is successful in driving the culture, this will influence non-management employees to be in line with the culture portrayed by management, which in turn should be in line with the IS strategy and policies.

  In this organisation, there were no significant differences indicated by the ANOVA tests between the job levels on the mean; therefore, no subculture was identified from a job level perspective. In other organisations, IS subcultures might be identified between job levels, but this should first be established through an analysis of the data. One could assume that management was successful in driving the IS culture from a job level perspective. This is supported by individual statements by employees (86.2%) who indicated that executive and senior managers demonstrated commitment to IS..

Furthermore, 86.7% of employees believed that managers perceived IS as important and 83.1% believed that executives perceived IS as important. 88.4% of employees felt that managers in their division appeared to adhere to the IS policy. These perceptions of employees towards management are strong cornerstones to support the fostering of a strong IS culture. This indicates that management is demonstrating their commitment and leading by example, which could explain why there are no significant differences between job levels.

- **Worked in information technology (IT) versus did not work in IT (non-IT) biographical groups:** Employees who worked in IT were significantly more positive towards IS than employees who did not work in IT in all four assessments. This means that the overall mean of employees who worked in IT was significantly higher than employees who did not work IT, as indicated through the t-test. For example, in 2013, the mean of the employees who worked in IT was 3.99, which is significantly more positive compared to the mean of those employees who did not, 3.88, based on the t-test analysis. There were two distinct groups of employees, each with a unique IS culture, which can be regarded as IS subcultures. These IS subcultures each had their own unique way of doing things when processing information and applying IS controls and processes.

  IT employees, for instance, had a better understanding of what an IS incident was (92.4%) than non-IT employees (86.8%). IT employees indicated that the IS policy was practical (85.6%), whereas non-IT employees were less positive (79.1%) in this regard, with only 69.25% of non-IT employees indicating that the policy was easy to understand compared with 74.8% of IT employees. To manage and change the IS culture of the non-IT employees, customised action plans should be developed. With IT employees having a stronger IS culture, the non-IT group should be targeted and interventions and resources prioritised accordingly. Should the same programme be used for both groups, either resources for the IT employees would be over-invested, or the critical risks as identified for the non-IT employees might not be covered. This could result in change not being instituted effectively and the IS culture not being positively influenced for employee groups where change is required.

- **Office locations – biographical groups:** The twenty-two office locations (A to V) are listed in no particular order in the first column. In some countries, there was more than one office, such as South Africa and the United Kingdom. In order to analyse the data of each office separately, the data of the countries was not grouped. This aids in determining if there is a difference in the IS culture across the various office locations.

  Most of the significant differences between biographical groups were identified between the office locations where the organisation operates. This could be explained by the fact that the offices are spread across geographical areas, each with its own country IS officer, IT managers and personnel per office, different schedules for IS training and unique IS problems. This confirms the creation of IS subcultures across the office locations where the organisation operates. For example, in the 2013 data, the Australia office (4.04), UK-London office (4.05) and SA-Johannesburg office (4.07) have a significantly lower mean score than the Mauritius office (4.49), Zurich office (4.35), Guernsey office (4.34), SA-Durban office and Pietermaritzburg office (4.22), UK-Manchester office (4.2), UK-Reading office (4.18) and Ireland office (4.17). This indicates that there is a group of offices where the IS culture is strongly shared, a group where the IS culture is apparently not shared and a group of offices where the IS culture is moderately shared. This indicates that the IS culture level varies between these geographically dispersed office locations (as indicated through the ANOVA tests) and thus each has unique aspects that must be addressed through interventions.

For example, the two office locations with the highest mean can be compared with the two office locations with the lowest mean. In the Australia office 55.3% and in the London office 69.2% of employees had read the IS policy. When comparing this with the significantly more positive office locations, it was found that in the Mauritius office 84.6% had read the IS policy and in the Zurich office 86.5% had done so. Therefore management can prioritise interventions for the Australia and London offices to motivate employees to read the IS policy.

Another example is that 58.4% employees from the Australia office and 62.5% from the London office, 84.6% from the Mauritius office and 80% from the Zurich office were informed of IS changes in a timely manner. If management is aware of areas where IS changes are not being communicated effectively, they can factor this into their project and change management plans for offices where employees perceive this aspect negatively. This will help employees become part of the changing process, enabling them to embrace change more positively.

There were a number of instances where significant differences were identified between the office locations of the case study organisation. The interventions per office location will not necessarily be similar, but should be aligned with each office's unique IS subculture. In the case study even offices within the same country had different subcultures, meaning that management should use different strategies to improve the IS culture issues of each office.

It is important to note that the IS culture mean scores for each of the individual biographical areas reveal an upward trend from the 2006 assessment to the 2013 assessment, indicating a change to a more positive IS culture over time, which could be related to the focused interventions per subculture (office location and people who worked in IT or not). Biographical areas where no significant differences were identified, for example the office locations that are not coloured in the table, can be referred to as the dominant IS culture as they represent the majority of the employees with no significant difference between the areas.

In this case study IS subcultures were identified between employees who worked in IT and those who did not, as well as between certain office locations. This might not be the case for all organisations as the IS culture could vary between them. In other organisations there might be significant differences between genders, age groups or nationalities. However, the biographical questions should be included to segment the data between the groups in order to use the ANOVA tests to identify significant differences which would be an indication of prevailing subcultures.

8.2 Phase 2: Planning interventions for improvement

8.2.1 Dominant culture interventions

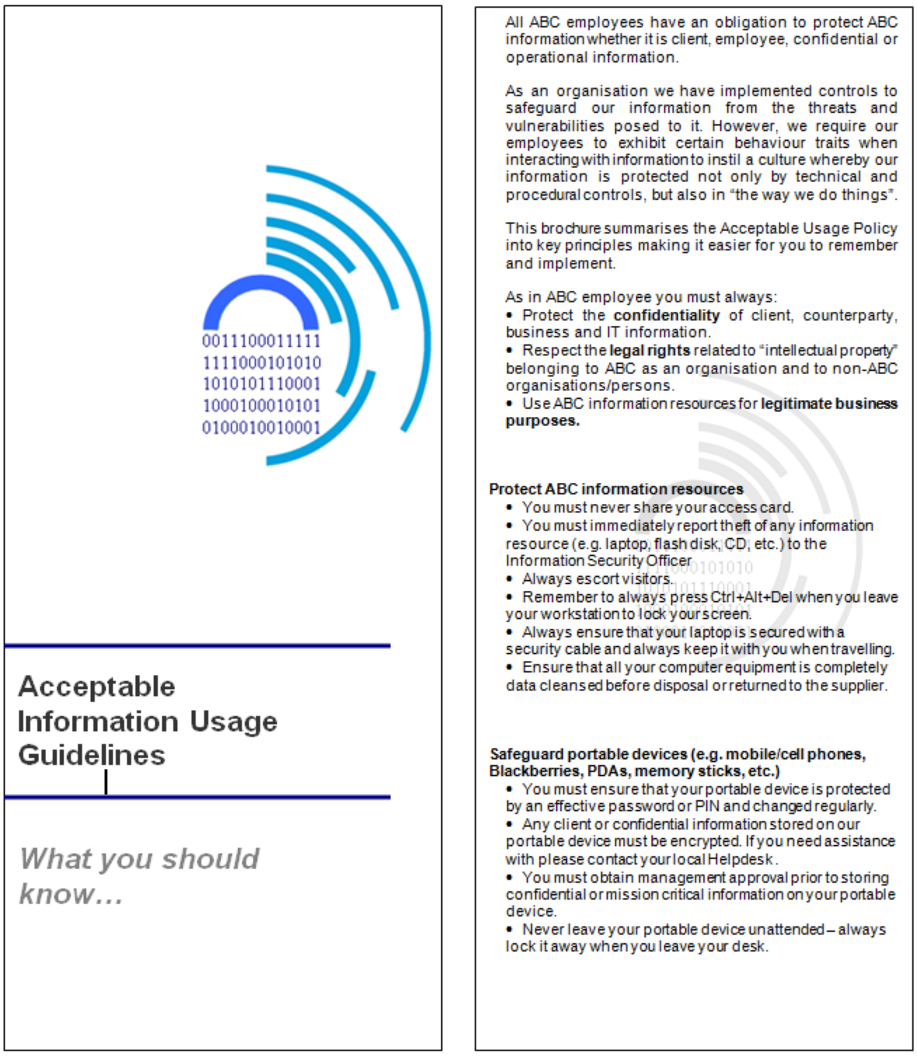
The statements with the lowest score on the overall mean were identified in each survey interval that was conducted. For each of the identified statements, a specific intervention was identified to be implemented across the organisation. Table 7 includes an extract of three of the lowest statements of the 2006 survey, the percentage employees that agreed, a summary of the interventions that were implemented as well as the 2013 percentage employees that agreed. The improvement in the "% agreement" indicates the improvement for each statement over the period after the specific interventions were implemented by the GISO.

The Acceptable Information Usage Guidelines brochure was compiled to address the last two statements in Table 7 relating to the communication and understanding of the IS policy. This brochure was developed and deployed across the organisation. Figure 2 presents the first two pages of the brochure that was sent out to employees.

Statements	2006 % agreement	Specific interventions that were conducted	2013 % agreement
I believe that third parties who have access to confidential ABC information preserve the confidentiality thereof.	42.6	Review policies and procedures to ensure that they meet the requirements when using third parties to process personal information on behalf of ABC. Ensure that third-party contracts are in place specifying security and privacy requirements by reviewing and updating the contracts as required. Include a discussion in the employee training about third-party security requirements of ABC to make employees aware of them. Ensure that third parties are aware of the requirements by conducting awareness campaigns.	49.70
The contents of the information security policy were effectively communicated to me.	51.4	Use preferred channels as indicated by employees, i.e. e-mail, presentations as well as web-based training to communicate the contents of the IS policy.	68.50
The contents of the information security policy are easy to understand.	55.1	Implement regular communication about IS policy requirements and changes, e.g. e-mails and posters, an Acceptable Information Usage Guidelines brochure and face-to-face presentations to employees about the policy contents.	70.1

Table 7: Extract of dominant culture interventions and improvement in % agreement

E-mails were sent out on a monthly basis after each survey. The themes of these e-mails were based on the concepts identified in the survey where interventions were required. The e-mail in Figure 3 relates to the survey statement in 2006 where only 28% of employees knew who the GISO was and 34.1% knew who their business unit security coordinator was. This improved to 44.6% for the GISO and 39.7% for the IS coordinators in 2013.


0011100011111
1111000101010
1010101110001
1000100010101
0100010010001

Acceptable Information Usage Guidelines

What you should know…

All ABC employees have an obligation to protect ABC information whether it is client, employee, confidential or operational information.

As an organisation we have implemented controls to safeguard our information from the threats and vulnerabilities posed to it. However, we require our employees to exhibit certain behaviour traits when interacting with information to instil a culture whereby our information is protected not only by technical and procedural controls, but also in "the way we do things".

This brochure summarises the Acceptable Usage Policy into key principles making it easier for you to remember and implement.

As in ABC employee you must always:

- Protect the **confidentiality** of client, counterparty, business and IT information.
- Respect the **legal rights** related to "intellectual property" belonging to ABC as an organisation and to non-ABC organisations/persons.
- Use ABC information resources for **legitimate business purposes.**

Protect ABC information resources

- You must never share your access card.
- You must immediately report theft of any information resource (e.g. laptop, flash disk, CD, etc.) to the Information Security Officer
- Always escort visitors.
- Remember to always press Ctrl+Alt+Del when you leave your workstation to lock your screen.
- Always ensure that your laptop is secured with a security cable and always keep it with you when travelling.
- Ensure that all your computer equipment is completely data cleansed before disposal or returned to the supplier.

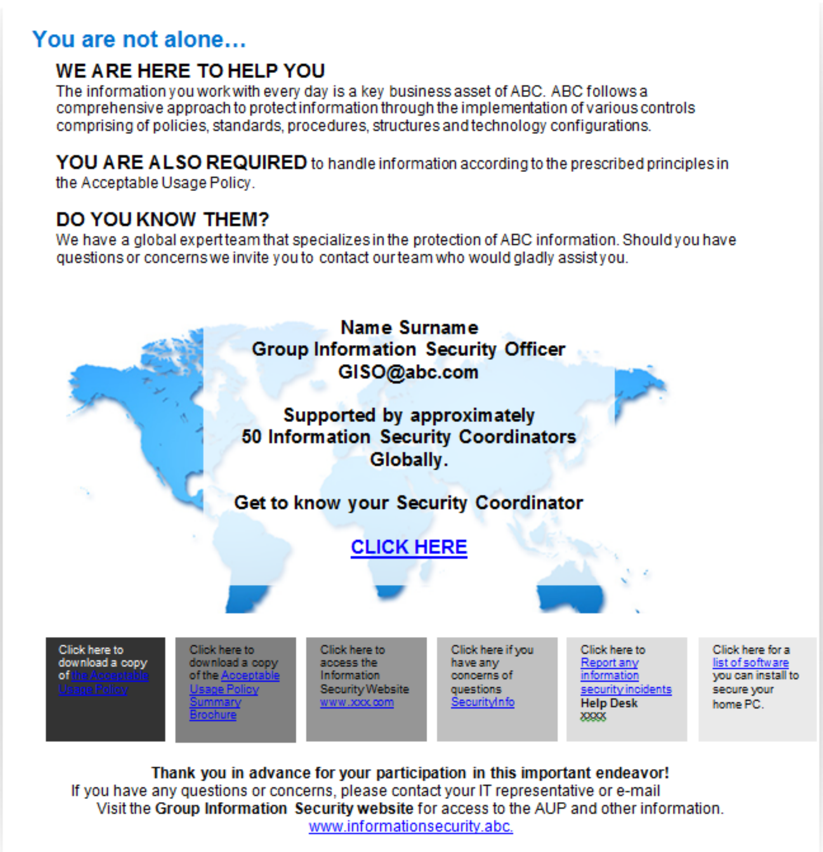
Safeguard portable devices (e.g. mobile/cell phones, Blackberries, PDAs, memory sticks, etc.)

- You must ensure that your portable device is protected by an effective password or PIN and changed regularly.
- Any client or confidential information stored on our portable device must be encrypted. If you need assistance with please contact your local Helpdesk.
- You must obtain management approval prior to storing confidential or mission critical information on your portable device.
- Never leave your portable device unattended – always lock it away when you leave your desk.

Fig. 2: Acceptable Information Usage Guidelines brochure

In 2006 only 54.6% of the respondents indicated that they had read the IS policy and only 65.2% knew where to get a copy of it. The location of where to download a copy of the IS policy was included on all e-mails and in the brochure. In 2013, 64.1% of the respondents indicated that they had read the policy and 70% knew where to get a copy, which was a significant improvement.

It is important to note that the e-mail topics, face-to-face presentation contents and messages of other communication channels used were adjusted after each survey, depending on which statements in the survey had the lowest score.



You are not alone…

WE ARE HERE TO HELP YOU
The information you work with every day is a key business asset of ABC. ABC follows a comprehensive approach to protect information through the implementation of various controls comprising of policies, standards, procedures, structures and technology configurations.

YOU ARE ALSO REQUIRED to handle information according to the prescribed principles in the Acceptable Usage Policy.

DO YOU KNOW THEM?
We have a global expert team that specializes in the protection of ABC information. Should you have questions or concerns we invite you to contact our team who would gladly assist you.

Name Surname
Group Information Security Officer
GISO@abc.com

Supported by approximately
50 Information Security Coordinators
Globally.

Get to know your Security Coordinator

CLICK HERE

Click here to download a copy of the Acceptable Usage Policy

Click here to download a copy of the Acceptable Usage Policy Summary Brochure

Click here to access the Information Security Website www.xxx.com

Click here if you have any concerns of questions SecurityInfo

Click here to Report any information security incidents Help Desk xxxx

Click here for a list of software you can install to secure your home PC.

Thank you in advance for your participation in this important endeavor!
If you have any questions or concerns, please contact your IT representative or e-mail
Visit the **Group Information Security website** for access to the AUP and other information.
www.informationsecurity.abc.

Fig. 3: IS awareness e-mail

8.2.2 IS subculture interventions

Table 8 presents an extract of two statements with a summary of the interventions that were identified. The percentage employees that agreed is based on the overall data, i.e. the dominant culture. The IS subcultures to target are listed in the last column, in order of priority, as indicated through the ANOVA tests. For this extract of the results, the office locations are portrayed under the biographical groups that had to be prioritised. The table outlines the specific interventions in column 4 that were defined after each of the surveys for the specific statements.

Questionnaire statement	**Survey year**	**% agreement**	**Dominant culture interventions**	**Biographical groups to prioritise (IS subcultures)**
The contents of the information security policy are easy to understand.	2013	70.1	Update brochure for all employees with a summary of the policy contents. Conduct face-to-face training in each country.	Australia – Sydney office South Africa – Johannesburg office United Kingdom – London office
	2010	69.2	Update brochure for all employees with a summary of the policy contents. Conduct face-to-face training in each country.	Australia – Sydney office South Africa – Johannesburg office
	2007	66.6	Ensure that all new employees attend induction training where information security is discussed. Explain the contents of the policy per job level. Design a brochure for all employees with a summary of the policy contents. Conduct face-to-face training in each country.	Australia – Sydney office South Africa – Johannesburg office South Africa – Cape Town office South Africa – Pretoria Office
	2006	55.1	Implement an IS training and education programme (course).	South Africa – Johannesburg office South Africa – Cape Town office

			Conduct face-to-face training in each country (indicated in survey as most preferred method of training).	United Kingdom – London office
The contents of the information security policy were effectively communicated to me.	2013	68.5	E-mails still most preferred method of communication (86.3%), followed by presentations (26.5%). Therefore continue to use it as communication channel. **Extract of topics** Location of policy (70.0% know) Who the GISO is (39.6% know). Controls implemented to ensure survival of business (67.0% believe business will survive a disaster).	Australia – Sydney office South Africa – Johannesburg office United Kingdom – London office
	2010	68.1	After e-mails (88.4), presentations (25.0) remain the most preferred method of communication. Therefore continue to use them as a communication channel. **Extract of topics** Location of policy (67.8% know). Who the GISO is (39.6% know). Controls implemented to ensure survival of business (64.9% believe business will survive a disaster).	Australia – Sydney office South Africa – Johannesburg office
	2007	66.0	SMS and discussion group preference for communication decreased. Web-based training increased – focus on inclusion of web-based training (7.2% to 11.1%). Presentations preference also increased from 17.5% to 23.5%. ISO to conduct presentations in each country. **Extract of topics** Location of policy (67.5% know). Who the GISO is (39.6% know). Controls implemented to ensure survival of business (60.6% believe business will survive a disaster).	Australia – Sydney office South Africa – Johannesburg office South Africa – Cape Town office South Africa – Pretoria Office
	2006	51.3	Send out monthly e-mail updates about policy contents. Use monthly posters, newsletter and presentations to communicate IS policy content and updates. **Extract of topics** Location of policy (65.2% know). Who the GISO is (28% know). Controls implemented to ensure survival of business (60.5% believe business will survive a disaster).	South Africa – Johannesburg office South Africa – Cape Town office United Kingdom – London office

Table 8: Extract of dominant culture interventions and biographical groups to prioritise

Apart from prioritising the IS subcultures to target, based on the overall results additional interventions were identified for the IS subcultures. In this case study, certain office locations were identified as IS subcultures and hence interventions were defined for each office location that was significantly more negative as identified through the ANOVA test. The results of the Australia – Sydney (identified in three of four surveys as a subculture) and South Africa - Johannesburg (identified in all four surveys as a subculture) are discussed to illustrate how the interventions were defined.

Face-to-face presentations were conducted by the GISO after each survey. The GISO planned visits to each country, including South Africa and Australia, throughout the year and coordinated the presentations with other project activities in those countries. The presentations were customised for each location based on the statements that required interventions. Listed below are the lowest five statements of 2006 that were addressed in the presentations for the Australia - Sydney office. The score for each statement improved from the 2006 to the 2013 survey.

1. Information security should be part of my performance development programme (PDP). (2006 - 49.4%, 2013 – 56.0%)
2. I believe that third parties who have access to confidential ABC information preserve the confidentiality thereof. (2006 - 49.4%, 2013 - 50.3%)
3. The contents of the information security policy were effectively communicated to me. (2006 - 51.9%, 2013 – 61.1%)
4. I am informed in a timely manner as to how information security changes will affect me. (2006 - 51.9%, 2013 – 58.4%)
5. I believe my division commits enough money to information security. (2006 - 52.6%, 2013 - 58.1%)

Aspects that were specifically addressed in the South Africa – Johannesburg presentations after the 2006 survey are listed below with the 2006 and 2013 percentage agreement. The score for each of these statements also improved from the 2006 to the 2013 survey.

1. I believe my division commits enough money to information security. (2006 - 38.1%, 2013 - 56.1%)
2. I believe my division commits enough people to information security. (2006 - 40.2%, 2013 – 58.1%)
3. I believe that third parties who have access to confidential ABC information preserve the confidentiality thereof. (2006 - 40.3%, 2013 – 44.8%)
4. The contents of the information security policy were effectively communicated to me. (2006 - 43.7%, 2013 - 63.0%)
5. I believe ABC’s employees adhere to the information security policy. (2006 - 47.0%, 2013 – 63.7%)

Table 9 portrays the overall mean and percentage agreement of the Johannesburg and Sydney offices. For both offices the overall mean also improved from 2006 to 2013.

Office location		**2013**	**2016**
South Africa - Johannesburg	Mean	3.85	4.07
	% agreement	72.7	81.6
Australia - Sydney	Mean	3.97	4.04
	% agreement	72.7	81.6

Table 9: Improvement of South Africa – Johannesburg and Australia – Sydney office mean and % agreement

The improvement in the individual statements as well as the overall mean illustrates the benefit of implementing targeted interventions for subcultures.

8.3 Phase 3: Mobilising resources to put the plan into action

The GISO coordinated the intervention plan and personally conducted most of the face-to-face presentations when visiting the various offices. The IS coordinators were involved in office-specific implementations, such as reviewing of third-party contracts or answering queries from the helplines. Outside consultants were also used to develop some of the awareness material based on the survey data and analysis.

8.4 Phase 4: Evaluating the effects

Once the interventions had been implemented, a follow-up survey was conducted using ISCA. The data of the previous ISCA could be compared with the follow-up survey data to establish whether the implemented actions had a positive impact on the IS culture. A follow-up ISCA also provided insight into whether the identified activities were successful and whether other developmental areas arose over time. This allowed for a longitudinal study to compare the data of the four surveys to establish if the IS culture improved over time. A comparison of the results of each survey is presented in Tables 5 and 6.

9. Discussions and limitations

Managing the IS culture is an ongoing process and the culture must be monitored on a consistent basis, benchmarked to previous assessments and directed to institute change. The process of managing and influencing an IS culture can be more successful if subcultures are identified and interventions are targeted at IS subcultures that are significantly more negative than other employee groups. IS subcultures were identified mainly across the geographically separated office locations of the case study organisation using statistical analysis. IS subcultures were also identified between employees who worked in IT and those who did not. As is evident from the data, subcultures were identified across all four assessments of the ISCA, illustrating how to identify IS subcultures (part of the second research objective). The biographical questions in the questionnaire were limited to those listed in this research based on the specifications of the organisation. However, other subcultures could exist between genders, language groups, generation groups, length of service groups or even permanent versus contract employees. It could be beneficial if organisations identified subcultures relating to the business structure and other demographic factors to further aid them in managing the IS culture of subculture groups. Future research will incorporate more biographical factors such as the generation groups to further explore the concept of subcultures.

The IS culture improved from 2006, with the most positive results in 2013, illustrating that a stronger IS culture develops over time if IS subcultures are identified with corresponding interventions. Focused action plans were developed for the biographical groups and prioritised from the lowest to the best scored subculture. The dominant IS culture and subculture results improved positively over time in line with the customised action plans that were implemented. The specific action plans related to aspects such as improving the policy contents and awareness and training initiatives. Implementation was prioritised, starting with the lowest scored subculture groups. This addressed the research objective to establish if there is an impact on IS subcultures if focused interventions are implemented.

Through targeted interventions the subcultures identified can be improved to be more closely aligned with the expected dominant culture to improve the overall IS culture to an acceptable level. The metrics derived can be used to gain insight into the security risk exposure of an organisation by including the results as part of an audit of the current IS risk and highlighting high-risk subcultures. The IS culture status in an organisation can furthermore provide insight into decision-making from a human perspective in incident management of the various subcultures, which could be integrated into incident response decision frameworks. In cases where the dominant IS culture or certain IS subcultures improve or become more positive, it illustrates that a more positive perspective of IS has been developed in line with IS strategies and policies. This will also enable management to identify and compare any differences in subcultures which might be present. The data can be benchmarked against previous assessments to determine change in the culture, to identify if awareness and training were successful or even to motivate for budget or resources for corrective actions required. It can further serve as input to ethics and compliance reviews to illustrate that the culture of the workforce is progressively improving to protect information.

A limitation of this research study is that changes in regulatory and contractual IS and data protection requirements over the period of the longitudinal study were not considered as the organisation used in the study has a global IS and privacy policy that all offices have to comply with. The influence of regulatory and contractual IS and data protection requirements on the IS culture will be addressed in further research as the study expands to include data from more companies that operate across various data protection and legal jurisdictions. The approach to measure the IS culture only included quantitative research methods using ISCA. Further research will explore the incorporation of qualitative research methods.

10. Conclusion

The first objective of this research was to understand the concept and development of dominant IS and subcultures. A dominant IS culture was defined as the IS values, perceptions and policy principles are shared by the majority of the organisation's members. An IS subculture was defined as a distinctive group of employees that share IS values, perceptions and policy principles that deviate from those shared by the majority of the organisation's members. The development of a dominant IS culture and subcultures was investigated by considering the development of an organisational culture together with various perspectives of researchers who have identified factors that influence IS culture. The IS culture develops as a result of the strategy and vision of management, which in turn influence the focus of the IS policy and direct employee behaviour, resulting in the dominant IS culture and subcultures. Extrinsic and intrinsic influences also play a role in influencing the IS culture and development of IS subcultures.

The second objective was to illustrate how to identify IS subcultures. As such the organisational development process is used to assess and identify the IS dominant and subcultures using an empirical approach with the Information Security Culture Assessment questionnaire. In the case study organisation, a number of subcultures were identified across the office locations and between employees that worked and did not work in IT. ANOVA and t-tests were used to identify the subcultures. Targeted interventions for the dominant IS culture and customised interventions for the identified subcultures were implemented. The overall means improved as did the individual statements illustrating the positive impact of targeting interventions per subculture

Organisations with offices across various locations, all working with the same level of confidential or personal information, need to ensure that IS controls are implemented and complied with consistently by employees across the organisation. If there are negative IS subcultures, it could introduce risk, however by identifying those IS subcultures, interventions can be identified to align it with positive IS subcultures that might exist. This research illustrated that IS subcultures are present in organisations. Once these subcultures are identified, management can target interventions for each subculture to positively influence the overall culture and to minimise the risk posed by certain subcultures in the organisation. Utilising the concept of subcultures, management can ultimately devise action plans to align opposing subcultures with the desired IS subcultures of the organisation.

Future research could explore how qualitative assessments can be used to identify and assess the dominant IS culture and subcultures. Additional empirical studies can be conducted to understand whether more subcultures exist across an organisation if data is segmented using more comprehensive demographic factors such as generation groups and gender. It would also be beneficial to compare the IS culture between different industries and sectors as more data is collected throughout the research project. This will allow a study of the impact of regulatory and contractual IS and data protection requirements across jurisdictions, which could also have an impact on the IS culture.

11. References

[1] Albrechtsen E (2007) A qualitative study of users' view on information security. Comput Secur 27:276-289

[2] Alfawaz S, Nelson K, Mohannak K (2010) Information security culture: a behaviour compliance conceptual framework. In: The Eighth Australasian Information Security Conference (AISC 2010) proceedings, Brisbane, pp 47–55

[3] AlHogail A (2015) Design and validation of information security culture framework. Comput Hum Behav 49:567–575

[4] AlHogail A, Mirza A (2015) Organizational information security culture assessment. In: The 2015 World Congress in Computer Science, Computer Engineering and Applied Computing (SAM'15) proceedings, Las Vegas, pp 287–292

[5] Alnatheer M, Nelson K (2009) A proposed framework for understanding information security culture and practices in the Saudi context. In: The 7th Australian Information Security Management Conference proceedings, Perth, pp 6-17

[6] Ashenden D (2008) Information security management: a human challenge? Inform Sec Tech Rep 13:195–201

[7] Ben-Asher N, Gonzalez C (2015) Effects of cyber security knowledge on attack detection. Comput Human Behav 48:51–61

[8] Berry ML (1997) Psychology at work, 2nd edn. McGraw-Hill Education, Dubuque

[9] Berry ML, Houston JP (1993) Psychology at work. Brown and Benchmark, WI

[10] Blaikie, N (2010) Designing social research, 2nd edn. Polity Press, Cambridge

[11] Box D, Pottas D (2013) Improving information security behaviour in the healthcare context. Procedia Tech 9:1093–1103

[12] Brewerton P, Millward L (2001) Organizational research methods. Sage, London

[13] Brijball S, Barkhuizen (2009) Organisational change and stress management. In: Robbins SP, Judge TA, Odendaal A, Roodt G (ed) Organisational behaviour, global and Southern African perspectives.

Pearson, Cape Town.

[14] Bryman A (2012) Social research methods, 4th edn. Oxford University Press, New York

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

[16] Byars LL, Rue LW (1997) Human resource management, 5th edn. McGraw-Hill, Boston

[17] Coghlan D, Brydon-Miller M (2014) The SAGE Encyclopaedia of Action Research. Sage, Los Angeles

[18] Da Veiga A (2015) The influence of information security policies on information security culture: illustrated through a case study. In: The Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015) proceedings, Lesvos, Greece, Plymouth University, pp 2–33

[19] Da Veiga A, Eloff JHP (2010) A framework and assessment instrument for information security culture. Comput Secur 29:196–207

[20] Da Veiga A, Martins N (2015) Improving the information security culture through monitoring and implementation actions illustrated through a case study. Comput Secur 49:162–176

[21] Dillon WR, Madden JT, Firtle NH (1993) Essentials of marketing research. Irwin, Boston

[22] Directive 95/46/EC (1995) EUR-Lex Access to European Law http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=celex:31995L0046 Accessed 22 August 2016

[23] Dojkovski S, Lichtenstein S, Warren M (2006) Challenges in fostering an information security culture in Australian small and medium sized enterprises. In: The 5th European Conference on Information Warfare and Security proceedings. Reading, England, Academic Conferences, pp 31–40

[24] Dojkovski S, Lichtenstein S, Warren MJ (2007) Fostering information security culture in small and medium size enterprises: an interpretive study in Australia. In: The European Conference on Information Systems (ECIS) proceedings, pp 1560–1571

[25] Dojkovski S, Lichtenstein S, Warren M (2010) Enabling information security culture: influences and challenges for Australian SMEs. In: The 21st Australasian Conference on Information Systems (ACIS) proceedings, Brisbane

[26] Flores R, Ekstedt M (2016) Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Comput Secur 59:26–44

[27] Flores WR, Antonsen E, Ekstedt M (2014) Information security knowledge sharing in organizations: investigating the effect of behavioral information security governance and national culture. Comput Secur 43:90–110

[28] Furnell S, Rajendran A (2012) Understanding the influences on information security behaviour. Comput Fraud Secur March: 12–15

[29] Furnell S, Thomson K (2009) From culture to disobedience: recognising the varying user acceptance of IT security. Comput Fraud Secur February: 5–10

[30] Gabriel T, Furnell S (2011) Selecting security champions. Comput Fraud Secur 11(8):8–12

[31] Hassan NH, Ismail Z (2012) A conceptual model for investigating factors influencing information security culture in healthcare environment. In: The International Congress on Interdisciplinary Business and Social Science 2012 (ICIBSoS 2012) proceedings, Procedia - Social and Behavioral Sciences, 65,

pp 1007–1012

[32] Heimes R (2016) Top 10 operational impacts of the GDPR: part 2 – The mandatory DPO. IAPP, The Privacy Advisor https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-2-the-mandatory-dpo/ Accessed 22 August 2016

[33] Hellriegel D, Slocum Jr, JW, Woodman RW (1998) Organizational behavior, 8th edn. South-Western College, Cincinnati, OH

[34] Herath T, Rao HR (2009) Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decis Support Syst 47:154–165

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

[36] Health insurance portability and accountability act. (HIPAA) (1996) U.S. Department of Health and Human Services (HHS) http://www.hhs.gov/hipaa/index.html Accessed 22 August 2016

[37] Hofstede G, Hofstede GJ, Minkov M (2010) Cultures and organizations: software of the mind, 3rd edn. McGraw-Hill, New York

[38] Hovav A, D'Arcy J (2012) Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the U.S. and South Korea. Inform Manage 49(2):99–110

[39] Hu Q, Dinev T, Hart P, Cooke D (2012) Managing employee compliance with information security policies: the critical role of top management and organizational culture. J Decision Sci Inst 43(4):615–660

[40] Ifinedo P (2014) Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. Inform Manage 51(1):69–79

[41] Information Security Forum (ISF) (2000) Information security culture – A preliminary investigation. S.I

[42] Institute of Directors in Southern Africa (IoDSA) (2009) King Code of Governance for South Africa (King III) from http://www.iodsa.co.za/?kingIII

[43] Johnson ME, Goetz E (2007) Embedding information security into the organization. IEEE Secur Privacy 5:16–24

[44] Karlsson F, Åström J, Karlsson M (2013) Information security culture – state-of-the art review between 2000 and 2013. Inform Comput Secur 23(3):246–285

[45] Knapp JK, Morris RF, Marshall TE, Byrd TA (2009) Information security policy: an organisational-level process model. Comput Secur 28:493–508

[46] Kraemer S, Carayon P, Clem J (2009) Human and organizational factors in computer and information security: pathways to vulnerabilities. Comput Secur 28:509–520

[47] Krejcie RV, Morgan DW (1970) Determining sample size for research activities. Educational and Psychological Measurement 30:607–610

[48] Kruger HA, Flowerday S, Drevin L, Steyn T (2011) An assessment of the role of cultural factors in information security awareness. In: The Information Security South Africa Conference (ISSA 2011) proceedings, Johannesburg, South Africa, pp 1–7

[49] Martin J (2001) Organisational behaviour, 2nd edn. Thomson Learning, London

[50] Martins N, Da Veiga A (2015) An information security culture model validated with structural equation modelling. In: The Ninth International Symposium on Human Aspects of Information Security &

Assurance (HAISA 2015) proceedings, Lesvos, Greece, Plymouth University, pp 11–21

[51] Martins E, Martins N (2016) Organisational culture. In: Robbins SP, Odendaal A, Roodt G (ed) Organisational behaviour, 3rd edn, Pearson Education, Cape Town, pp 606–641

[52] Martins N, Van der Ohe H (2006) Detecting sub cultures in an organisation. South Afr Bus Review 10(2):130–149

[53] Munteanu A, Fotache D (2015) Enablers of information security culture. Procedia Econ Financ 20:414–422

[54] Ngo L, Zhou W, Warren M (2005) Understanding transition towards information security culture change. In: The Australian Information Security Management Conference proceedings, Perth, Australia, pp 67–73

[55] Nosworthy JD (2000) Implementing information security in the 21st century – do you have the balancing factors? Comput Secur 19(4):337–347

[56] Organisation for Economic Co-Operation and Development (OECD) (2002) Guidelines for the Security of Information Systems and Networks. Towards a Culture of Security. OECD www.oecd.org/dataoecd/16/22/15582260.pdf Accessed 22 August 2016

[57] Padayachee K (2012) Taxonomy of compliant information security behavior. Comput Secur 31:673–680

[58] Parsons K, McCormac A, Butavicius M, Pattinson M, Jerram C (2014) Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Comput Secur 42:165–176

[59] Pheysey DC (1993) Organizational cultures, types and transformations. Routledge, London

[60] Protection of Personal Information Act (PoPI) 4 of 2013 (2013) http://www.acts.co.za

[61] Rossouw D, Van Vuuren L (2013) Business ethics, 5th edn. Oxford University Press, Cape Town

[62] Ruighaver AB, Maynard SB, Chang S (2007) Organisational security culture: extending the end-user perspective. Comput Secur 26:56–62

[63] Saunders M, Lewis P, Thornhill A (2009) Research methods for business students. 5th edn. Pearson, London

[64] Schein EH (1985) Organizational culture and leadership. Jossey-Bass, San Francisco

[65] Schein EH (2006) Cultures and organizations: software of the mind, 3rd edn. John-Wiley and Sons, San Francisco

[66] Schlienger T, Teufel S (2003) Analyzing information security culture: increased trust by an appropriate information security culture. In: The International Workshop on Trust and Privacy in Digital Business (TrustBus 2003) in conjunction with the 14th International Database and Expert Systems Applications (DEXA 2003) proceedings, Prague, Czech Republic

[67] Schlienger T, Teufel S (2005) Tool supported management of information security culture: an application to a private bank. In: The Security and Privacy in the Age of Ubiquitous Computing Conference proceedings, IFIP, Japan, pp 65–77

[68] Shameli-Sendi A, Aghababaei-Barzegar R, Cheriet M (2016) Taxonomy of information security risk

assessment (ISRA). Comput Secur 56:14–30

[69] Sherif E, Furnell S, Clarke N (2015) An identification of variables influencing the establishment of information security culture. In: Tryfonas T, Askoxylakis I (ed), The human-computer interaction (HCI) conference – human aspects of information security, privacy and trust (HAS), Switzerland, Springer, pp 436–448

[70] Shuchih EC, Chin-Shien L (2007) Exploring organizational culture for information security management. Ind Manage Data Syst 107(3):438–458

[71] Sarbanes-Oxley Act of 2002 (SOX) (2002) US Securities and Exchange Commission https://www.sec.gov/about/laws/soa2002.pdf Accessed 22 August 2016

[72] SPSS version 22 (2013) IBM Software Group, Chicago, IL

[73] Survey Tracker (2014) Survey Tracker https://www.surveytracker.com Accessed 22 August 2016

[74] Swire PP, Berman S (2007) Information privacy, official reference for the certified information privacy professional. IAPP, Portsmouth

[75] Thomson K, Von Solms R, Louw L (2006) Cultivating an organisational information security culture. Comput Fraud Secur October: 7–11

[76] Tsohou A, Karyda M, Kokolakis S (2015) Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. Comput Secur 52:128–141

[77] UK Corporate Governance Code (2014) Financial Reporting Company https://www.frc.org.uk/Our-Work/Publications/Corporate-Governance/UK-Corporate-Governance-Code-2014.pdf

[78] Van Niekerk J, Von Solms R (2005) A holistic framework for the fostering of an information security sub-culture in organizations. In: The Information Security South Africa Conference (ISSA2005) proceedings, Johannesburg, South Africa, pp 1–13

[79] Van Niekerk J, Von Solms R (2006) Understanding information security culture: a conceptual framework. In: The Information Security South Africa Conference (ISSA2006) proceedings, Johannesburg, South Africa

[80] Van Niekerk J, Von Solms R (2010). Information security culture: a management perspective. Comput Secur 29:476–486

[81] Vroom C, Von Solms R (2004) Towards information security behavioural compliance. Comput Secur 23(3):191–198

[82] Wilderom CPM, Van den Berg PT, Wiersma UJ (2012) A longitudinal study of the effects of charismatic leadership and organizational culture on objective and perceived corporate performance. Leadership Quart 23(5):835–848

[83] Yeats D, Cadle J (1996) Project management for information systems, 2nd edn. Pitman, London

[84] Zakaria O (2006) Internalisation of information security culture amongst employees through basic security knowledge. In: The International Conference on Information Security proceedings, Karlstad, Sweden, pp 437–441

[85] Zellmer-Bruhn ME, Gibson CB, Aldag RJ (2001) Time flies like an arrow: tracing antecedents and consequences of temporal elements of organisational culture. In: Cooper CL, Cartwright S, Earley PC (ed). The international handbook of organisational culture and climate. West Sussex: John Wiley & Sons, pp 21–52

[86] ISO/IEC 27002:2013 Information technology e-security techniques e-code of practice for information security management, BSI: Kay Westlake

[87] PricewaterhouseCoopers (2016) Global state of information security survey http://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf

[88] Ernest and Young (2015) Creating trust in the digital world, Global information security survey http://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2015-1

[89] Information Commissioner (2013) Privacy impact assessment and risk management https://ico.org.uk/media/1042196/trilateral-full-report.pdf

[90] Reynolds CA (2010) The identification of organisational subcultures in an international energy company, Thesis, Massey University, New Zealand.

[91] Trice HM, Beyer JM (1993) The cultures of work organisations. Prentice Hall, Englewood Cliffs

[92] Plunkett WR, Attner RF (1994) Introduction to management, 5th edn. Wadsworth, Belmont

[93] Hampton J (2015) Fundamentals of enterprise risk management, 2nd edn. Amacom, New York

[94] Knapp KJ, Morris RF, Marshall TE, Byrd TA (2009) Information security policy: an organizational-level process model. Comput Fraud Secur 28(2009): 493-508

[95] RSSB (2016) Safety culture toolkit http://safetyculturetoolkit.rssb.co.uk/safety-culture-information.aspx

[96] Fleming M (2000) Safety culture and maturity model. The Keil Centre. Crown, Norwich http://www.hse.gov.uk/research/otopdf/2000/oto00049.pdf

[97] Douglas M, Wildavsky A (1982) Risk and culture. University of California Press, Los Angeles

[98] Thompson M, Ellis R, Wildavsky A (1990) Cultural theory, Political culture series. Westview Press, San Francisco

[99] Ashkanasy NM, Broadfoot LE, Falkus S (2000) Questionnaire measures of organisational culture. In: Ashkanasy NM, Wilderom CPM, Peterson MF (ed) Handbook of organisational culture and climate, Sage, California

[100] Sabbagh BA, Kowalski S (2012) Developing social metrics for security
modeling the security culture of it workers individuals (case study). In: The 5th International Conference on Communications Computers and Applications (MIC-CCA2012) proceedings, Istanbul, Turkey, pp 112-118

[101] Smircich L, Morgan G (1982) Leadership: the management of meaning. J of Appl Behave Psych 68: 653-663

[102] Jones ML (2007) Hofstede – Cultural questionable? Oxford Business & Economics Conference. Oxford, UK.

[103] Oltedal S, Moen B, Klempe H, Rundmo T (2004) "Explaining risk perception. An evaluation of cultural theory", Rotunde no. 85. C Rotunde Publikasjoner, Norway.

[104] Martins N (2016) Organisational diagnosis. In: Martins N, Geldenhuys D (ed) Fundamentals of organisation development, Juta, Cape Town.

[105] Safa NS, Sookhak M, Von Solms R, Furnell S, Ghani NA, Herawan T (2015) Information security conscious care behaviour formation in organizations. Comput Secur 53:65-78

[106] Lavarkas PJ (2008) Research design. In: Lavarkas PJ (ed) Encyclopaedia of survey research methods http://0-dx.doi.org.oasis.unisa.ac.za/10.4135/9781412963947.n471

[107] Durand C (2016) Surveys and society. In: Wolf C (ed) The SAGE handbook of survey methodology, http://0-dx.doi.org.oasis.unisa.ac.za/10.4135/9781473957893.n5

[108] Faily, S, Fléchais, I (2010). Designing and aligning e-science security culture with design. Inf Man and Comput Secur 18(5):339-349.

[109] Huysamen, GK (1988) Sielkundige meting – ‘n Inleiding. Van Schaik, Pretoria.

[110] Nel M, Martins N (2014) Validating a theoretical model of organisational culture and occupational health by means of structural equation modelling In: The thirteenth European Conference on Research Methodology for Business Management Cass Business School, City University, London, 16-17 June.

[111] Jackalas MB, Martins N, Ungerer LM (2016) The impact of demographic variables on organisational culture and employee motivation: evidence from a health insurance company in Botswana. J of Contemp Ma, 13:257-384.