Accepted Manuscript (Unedited)

Appears in: *Computer Law & Security Review*

Adéle da Veiga, Nico Martins, Information security culture and information protection culture: A validated assessment instrument, *Computer Law & Security Review*, 31, 2015, Pages 243-256
http://dx.doi.org/10.1016/j.clsr.2015.01.005

Information Security Culture and Information Protection Culture: A Validated Assessment Instrument

ADÉLE DA VEIGA AND NICO MARTINS

Dr. A Da Veiga is with the College of Science, Engineering and Technology, School of Computing, University of South Africa, P.O. Box 392, UNISA 0003, South Africa (email: dveiga@unisa.ac.za)
Prof. N. Martins is with the Department of Industrial and Organisational Psychology, University of South Africa, P.O. Box 392, UNISA 0003, South Africa

Abstract

A strong information protection culture is required in organisations where the confidentiality, sensitivity and privacy of information are understood and handled accordingly. This is necessary to reduce the risk of human behaviour to the protection of information as well as to uphold privacy requirements from a regulatory perspective. This research explores the concept of an information security culture and how information privacy can be incorporated to define an information protection culture. Next, the researchers explain information attributes relating to information security and information privacy to derive information attributes that can be considered when referring to an information protection culture. The information attributes are used to evaluate an existing information security culture assessment instrument that can potentially be used to assess an information protection culture. The research reveals that the information security culture assessment (ISCA) instrument can be used, but that it can be further improved by incorporating additional privacy concepts. An information protection culture assessment (IPCA) is conducted as part of a case study in an organisation. This allowed for a factor and reliability analysis to validate the IPCA. The analysis indicated that the IPCA is valid and reliable when grouping the items into the newly identified factors, but can further be enhanced by aligning it to information privacy attributes.

Key words: information security, information security culture, information protection culture, privacy, personal information, assessment, behaviour, human, questionnaire

1 Introduction

The prevention of loss, damage, unauthorised destruction or access to information processed by organisations is an ongoing evolution. Internal and external risks continuously evolve and often result in breaches. In many instances, employee behaviour is the root cause of several information security incidents and privacy breaches (Herold 2011). A survey conducted by PricewaterhouseCoopers (2014) found that current employees (31%) and former employees (27%) still contribute to information security incidents. Interestingly, the survey results indicated that the number of actual incidents caused through employees has risen by 25% since the 2013 survey. Research conducted by the Ponemon Institute (2013) indicated that the root causes of breaches were related to human factors (35%), system glitches, (29%) and malicious or criminal attacks (37%).

Employee behaviour that results in security incidents and privacy breaches could be as a result of negligence, error, or a deliberate malicious attack. Guo (2013) classified employee behaviour in four categories namely, security assurance behaviour, security compliant behaviour, security risk-taking behaviour, and security damaging behaviour. The last two categories of employee behaviour could pose a risk to the protection of information. The security risk-taking behaviour is

for example not in line with the organisation's policies and may put the organisation's information at risk although it is unintentional. The security damaging behaviour is malicious, intentional and can cause direct damage to information. Liginlal, Sim and Khansa (2009) found in their research that slips and mistakes can result in privacy breaches. They concluded that the management of human error should be a high priority in organisations and propose an error management programme that deals with the root cause analysis of privacy incidents, a defence-in-depth strategy and periodic evaluation of operational and technical measures. Other researchers (Johnson and Goetz 2007, Padayachee, 2012) emphasised the importance of focusing on behavioural issues and building an information security culture when embedding information security in an organisation.

A strong information security culture can contribute in minimising the risk from employee behaviour when interacting with and processing information (Da Veiga & Eloff 2010). The culture in an organisation should be conducive to the protection of information. A culture is required in which employees comply with the information security policy and processing requirements. This will help to minimise risks from an employee perspective such as wrongful disclosure of sensitive information; unlawful usage of information; unauthorised transfer of information to third parties or outside of legal jurisdictions without the required controls; saving sensitive and/or confidential information in unencrypted format on mobile devices; using internet e-mail accounts to e-mail sensitive and/or confidential information; and infrequent back-ups resulting in inaccurate or lost information.

The information security policy and processing requirements of information are directed by a number of requirements such as international standards, regulatory and legal requirements, business objectives, the inherent risk of information, and so on. Regulatory and legal requirements are a critical corner stone of policies to direct the processing requirements of information and the controls to protect it. The applicable privacy legislation must be complied with when organisations process personal information. The term "information privacy" is often used to refer to the appropriate collection and handling of personal information (Swire & Bermann 2007). It is essential that privacy principles are also embedded in the information security culture to aid in meeting compliance and customer expectations when processing personal information. The culture in organisations should thus be conducive to the protection of information from an information security and privacy context. This will aid to minimise the risk of incidents caused by employees whether by negligence, error or deliberate malicious attacks when processing sensitive or personal information.

Introducing the concept of privacy has the implication that one cannot refer to an information security culture as such. A term is required that encompasses an information security culture as well as a culture where the principles of privacy becomes the way things are done in the organisation. This paper further explores the concept of defining such a culture, namely an information protection culture.

The paper further aims to identify whether a culture comprising of information security and privacy principles can be assessed or measured in order to monitor and improve it. Monitoring the culture is critical in order to shape it into one in which the nature, confidentiality and sensitivity of information is understood and handled accordingly by employees. One approach that can be used is an Information Security Culture Assessment (ISCA), developed in previous research (Da Veiga & Eloff 2007, Da Veiga & Eloff 2010, Da Veiga, Martins & Eloff 2007). ISCA can be used to aid management in reducing the risk that employee behaviour poses to the protection of

information and to ultimately inculcate a culture with fewer breaches resulting from an internal perspective. This research explores the ISCA instrument to determine whether it can be used to assess an information security culture whilst encapsulating privacy principles, in other words to assess an information protection culture.

2 Aim of this paper

The first aim of this paper is to introduce the concept of an information protection culture which encapsulates the concept of an information security culture and privacy principles.

The second aim is to establish if the ISCA instrument can be utilised to assess an information protection culture. This is explored by reviewing the ISCA instrument from an information privacy perspective. A case study is utilised to validate the ISCA instrument by conducting a factor and reliability analysis in order to propose an information protection culture assessment (IPCA) instrument.

The research deals with the following two main research questions:

- What is the difference between an information security culture and an information protection culture?
- Can the ISCA be used to assess an information protection culture?

The paper is structured as follows: In section 3 the concept of an information protection culture is defined. This is achieved by understanding what the attributes of information are and what influences the manner in which information is processed in an organisation. The terms "information security" and "information privacy" are discussed to further identify attributes of information to illustrate a holistic perspective on information. Next, the definition of "information security culture" is expanded to incorporate the concept of privacy and to define an "information protection culture".

In section 4 the ISCA assessment instrument is evaluated against the information attributes to establish whether it is comprehensive enough to assess an Information Protection Culture. The research methodology is discussed in section 5 and the implementation of it in the case study organisation is presented in section 6. This is followed by the validity and reliability analysis of the ISCA measurement instrument in section 7 and 8. A discussion on the research questions are provided in section 9 with conclusions and proposed future research in section 10.

3. Defining an Information Protection Culture

3.1 Information

The Infosecurity Europe 2014 Industry Report (2014) states that 2,5 billion gigabytes of data was generated on a daily basis in 2012. Data, being the plural of datum, is closely related to the term "information". The King III (2009) report defines information as, "Raw data that has been verified to be accurate and timely, is specific and organised for a purpose, is presented within a context that gives it meaning and relevance and which leads to increase in understanding and decrease in uncertainty". Information is thus, data that is analysed and presented in a context that derives value for organisations and individuals. Information is part of every business and is a valuable asset that must be protected (Breuning, Sotto, Abrams & Cate 2008). Organisations need to process information in order to derive value and ultimately meet the business and stakeholder

objectives. In addition information must be governed effectively to achieve social, environmental and sustainability performance (King III 2009).

Employees in organisations often have access to sensitive information such as social security numbers, tax numbers, credit card numbers or health information of customers or employees. The manner in which employees process and use the information is critical to prevent mistakes, misuse or incorrect disclosure, which could stem from ignorance, fraud or wilful damage.

To further understand information four vital **attributes** thereof are discussed below:

- Format: Information exists in various formats or mediums such written, electronic or digital, verbal, photographed, printed, painted, drawn, photographs, and so on.

- Categories: Each department in an organisation processes different categories of information such as financial information (eg credit card numbers, payslips, tax numbers, bank statements), health information (blood test results, prescriptions), personal information (eg social security numbers, address, racial or ethnic information) or intellectual property or strategies to mention but a few.

- Information life cycle: The processing of information could be in various phases of the information life cycle. Information collected from customers via application forms, call centres of via the internet is in the "collection phase". Once the information is collected it is stored in a database, cloud or other medium, referred to as the "storage phase". The collected data is then processed and used to deliver services, sell products, to do analysis and so on, being part of the "use phase". Information can also be "transferred" between business units, subsidiaries, third parties or cross border. As part of the "retention phase", information needs to be retained to meet business, industry, customer, legal and regulatory requirements. Information that is no longer used and that has met its retention periods are "archived" and at a certain point in time "destructed" in line with organisational policies and legal requirements (Herath 2011).

- Classification: Information can be classified according to its sensitivity in order to apply the appropriate controls to protect the information. Various classification schemes are available to classify information such as (Herath 2011, SOGP 2007):
    - top secret information (highly sensitive information that could have a material impact on the organisation should the confidentiality, integrity and/or availability (CIA) be affected)
    - confidential information (sensitive information that could result in a major impact on the organisation should the CIA be affected)
    - restricted information (internal information restricted to specific business units or users that could result in a moderate impact on the organisation should the CIA be affected)
    - public information (information that is available to employees and external parties with no impact if the CIA is affected)

Various internal and external factors influence the format, classification and categories of information that are processed through its life cycle by an organisation. The mission, vision, services, products, internal policies and procedures and technologies are for instance factors that

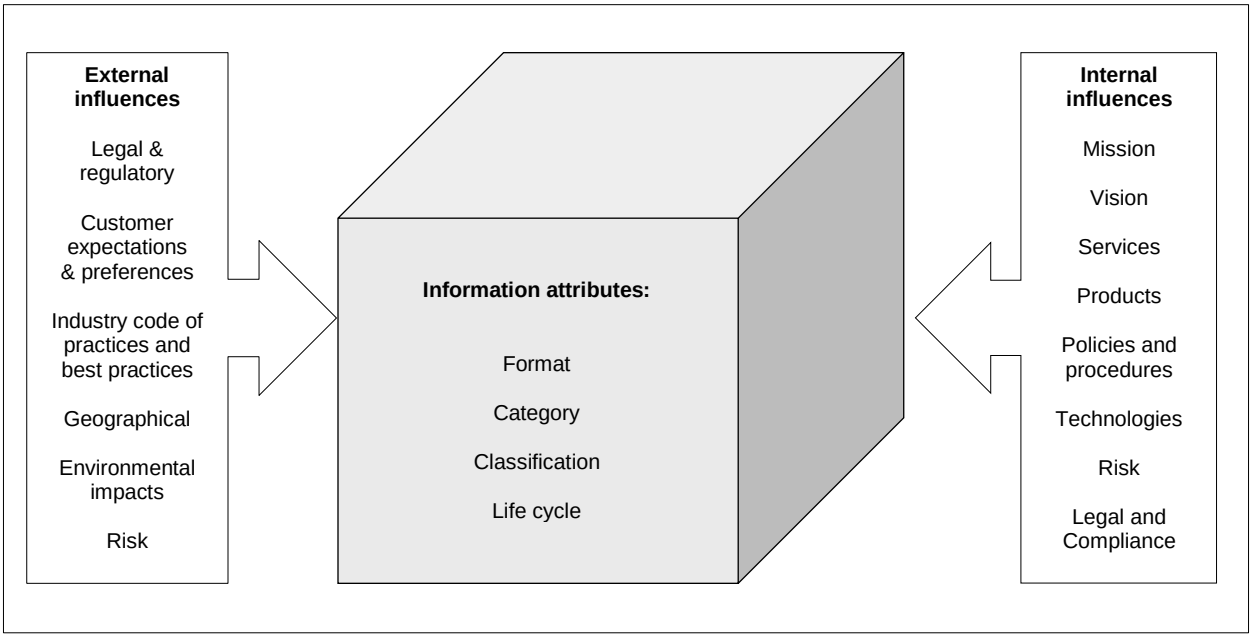
influence the attributes of information. A bank would for instance process financial and personal information of customers (category) which will be driven by various financial products. Internal policies will direct employees in terms of business processes and how to handle the customer's information through the information life cycle. Similarly, contractual requirements with customers or third parties outline terms and conditions that must be complied with in line with regulatory requirements. A Privacy Statement or Privacy Notice is an example of an agreement with customers, and even employees, which describes how the organisation will process personal information in line with regulatory requirements and to meet customer expectations. From an internal perspective organisations must ensure that compliance is monitored in line with external regulatory and internal legal and contractual requirements. Various technologies will be implemented to support the services and products offered to the customer such as internet and cell phone banking (format). The information can be in a hard copy and electronic format and will be classified according to its sensitivity. The sensitivity will direct the type of controls to implement in order to protect the information through its life cycle in the various formats.

Similarly external factors influence the attributes of information. External factors such as regulatory requirements, customer expectations and preferences, best practices, geographical distribution, environmental impacts and so on, affect what and how information is processed. For example, if financial information about customers is processed, a number of regulatory requirements would apply, such as the regulation protecting personal and financial information. This could for instance place requirements on the approval process for loans or how long to keep customer records. Customers could have their own preferences of how their personal information should be handled, for example if it can be shared with third parties for marketing purposes or not. Best practice standards provide guidelines to organisations such as the ISO/IEC 27002 (2013) for information security management. The Payment Card Industry Data Security Standard (PCI DSS 2010) will for example apply if cardholder information (eg debit and credit cards) is processed.

Geographical influences refer to regional or global disbursements of business operations and the processes in place to share information across borders using various technologies such as video conferencing, dropbox, intranet, e-mail, etcetera. Environmental influences could relate to health and safety requirements such as medical checks for employees where health information will be processed. Various external risks influence the manner in which information is processed. For example, the likelihood and impact of threats such as hackers, viruses, industrial espionage or environmental risks would impact how information is processed, in other words whether it is encrypted, backed up in various locations, and so on. Internal risks such the risk of employee error could influence the processing of information to be part of a process whereby captured data is verified and signed-off prior to final processing.

Figure 1 illustrates the attributes of information as well as examples of possible external and internal influences that impact on what and how information is processed in an organisation.

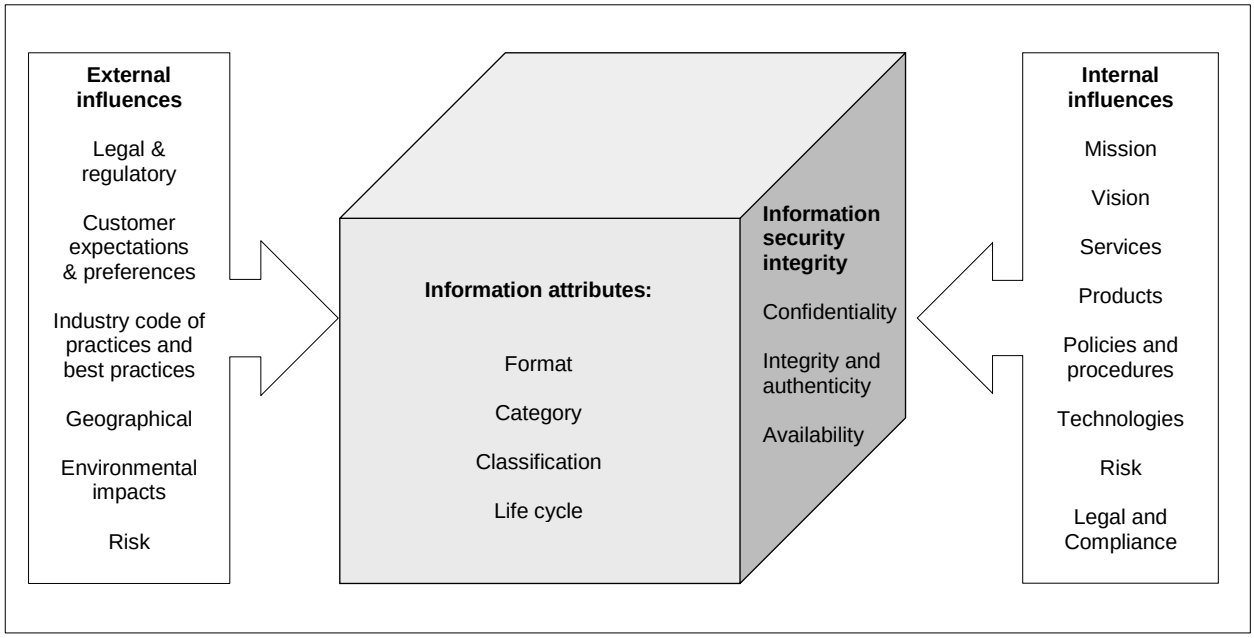
Figure 1: Information attributes and influences.



3.2 Information security

Information that is processed by an organisation must be protected to ensure that its confidentiality and integrity are maintained and that it is readily available (CIA) when needed to minimise the possibility of harm that could be caused to a business (FIRM). Information security is concerned with the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction (King III, 2009). It preserves the confidentiality (preventing unauthorised use to access information), integrity and authenticity of information (ensuing the completeness, accuracy and validity of information), availability (ensuring that information could be accessed at all times) of information whilst considering its authenticity, accountability, non-repudiation and reliability (ISO/IEC 27002 2013). The objective is to protect information from threats that impact on the continuity of the business and to ultimately maximise return on investments and business opportunities. (King III, 2009). The CIA of information is depicted in figure 2 as a second set of attributes that must be considered in terms of information.

Figure 2: Information attributes and influences with information security



3.3 Information privacy

Organisations process information about employees, customers, business partners, patients, or students. The information could relate to only their names and addresses, but often includes social security numbers, credit card numbers, bank account details, health information or even information on children. If the information is accessed or disclosed to unauthorised parties if could lead to fines, civil proceedings or even jail sentences from a regulatory perspective; furthermore the organisation's reputation could be damaged; it could lead to financial loss or even identity theft for the individuals affected by the incident. As an example, one of the worst data breaches related to the Heartlands Payment System where information of 134 million credit cards was exposed in 2008. It is estimated that Heartland costs associated with the breach, fines and remediation costs amounted to $12,6 million in 2009. Their stock price fell with 80% during this period and one of the reasons for the decline was related to the data breach. The hacker who was involved in the data breached received a prison sentence of 20 years (Zurich 2009).

This type of information is called "personal identifiable information" (PII) or "personal data" and the processing thereof is legislated in many countries through privacy laws. The OECD (1980) defines personal data as, "personal data" means any information relating to an identified or identifiable individual (data subject)". The EU Directive 95/46/EC, defines personal data as, "any information relating to an identified or identifiable natural person ('data subject')". Personal information is defined by the Protection of Personal Information Act 4 of 2013 (PoPI 2013) of South Africa as, "information relating to an identifiable, living, natural person and where it is applicable, an identifiable, existing juristic person". The South African privacy law includes reference to juristic persons, which is typically not included in most other jurisdictions. For the purpose of this study the term "personal information" will be used.

According to Greenfield (2014), in June 2013, there were 99 countries with privacy laws and about 20 governments in the process of considering such a law. In November 2013, South Africa's Protection of Personal Information Act 4 of 2013 (PoPI) was promulgated and a number of other countries followed.

The concept of privacy goes back as far as 1948 where human rights were defined in the UN Universal Declaration of Human Rights (UN 1948). In 1970, the US Department of Health, Education and Welfare (today referred to as Department of Health and Human Services) developed the Code of Fair Information Practices (Swire & Berman 2007). The Organisation of Economic Cooperation and Development (OECD) published guidelines on the protection of personal information and trans-border flows of personal data in 1980 (OECD 1980) which the US Federal Trade Commission (FTC) endorsed. The USA adopts a sectoral approach to privacy with privacy regulations per industry, for example, the financial or medical sector (Swire & Berman 2007). In Europe, the EU Data Directive 95/46/EC came into effect in 1998, and outlined privacy principles to protect the privacy of individuals and to facilitate the free flow of personal data within the European Union (EU Data Directive 95/46/EC 1995). The EU Privacy Directive is currently being revised to formulate a regulation that will apply to all European member states (EC 2014). The Asia Pacific Economic Cooperation (APEC) Privacy Framework was established in 2005 (APEC 2005). In Africa alone, there are 15 countries with privacy related laws and five countries in which privacy protection efforts are under way.

The OECD (1995) privacy principles are enshrined in most of the privacy laws, and focus on the following as adapted from the OECD (1995):

- Collection limitation: Responsible parties (i.e. a public or private body or any other person which defines the purpose and means for processing personal information, PoPI 2013), should limit the collection of personal information. Personal information should only be collected lawfully and fairly and, where appropriate, with the knowledge or consent of the data subject. Organisations should therefore not collect more information about their customers than what is required. If it is not necessary to collect information about the customer's children, ethnic background or criminal information to provide a service or product to the customer, then it should not be collected. Information should also not be collected without the customer's knowledge by way of, for instance CCTV, unauthorised purchases of databases with personal information or websites where more personal information is collected than necessary and shared with other parties.

- Data quality: Personal information that was collected should be relevant to the purposes for which responsible parties want to process it and in addition the personal information should be accurate, complete and be kept up-to-date. This principle relates to the integrity of data whereby processes should for instance be in place to verify data capturing as well as updating it when a customer for instance changes his family name or relocates.

- Purpose specification: The purposes for which personal information are collected by responsible parties should be specified at the time of the collection, where possible. The subsequent use of the personal information should be limited to those purposes. Apart from specifying the purpose in contractual documents and business processes, the responsible party should ensure that employees do not use personal information for any other purpose as agreed with the customer. Purpose specification is often encapsulated in

privacy notices and customers should be provided with opportunity to opt-in for certain processing such as marketing.

- Use limitation: Personal information should not be disclosed, made available or otherwise used for purposes except with the consent of the data subject or by the authority of law. Organisations should ensure that consent is obtained for any further processing and for instance also remain accountable for third parties that have access to the personal information of the responsible party. This implies that appropriate information security controls should also be in place to protect personal information from unauthorised disclosure.

- Security safeguards: Personal information should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data. Security safeguards should be appropriate to the related risk of the personal data in its various formats, categories and information life cycle phase. The security safeguards for instance include risk assessments, information security policies, privacy by design – when developing software or systems, IT auditing and online privacy.

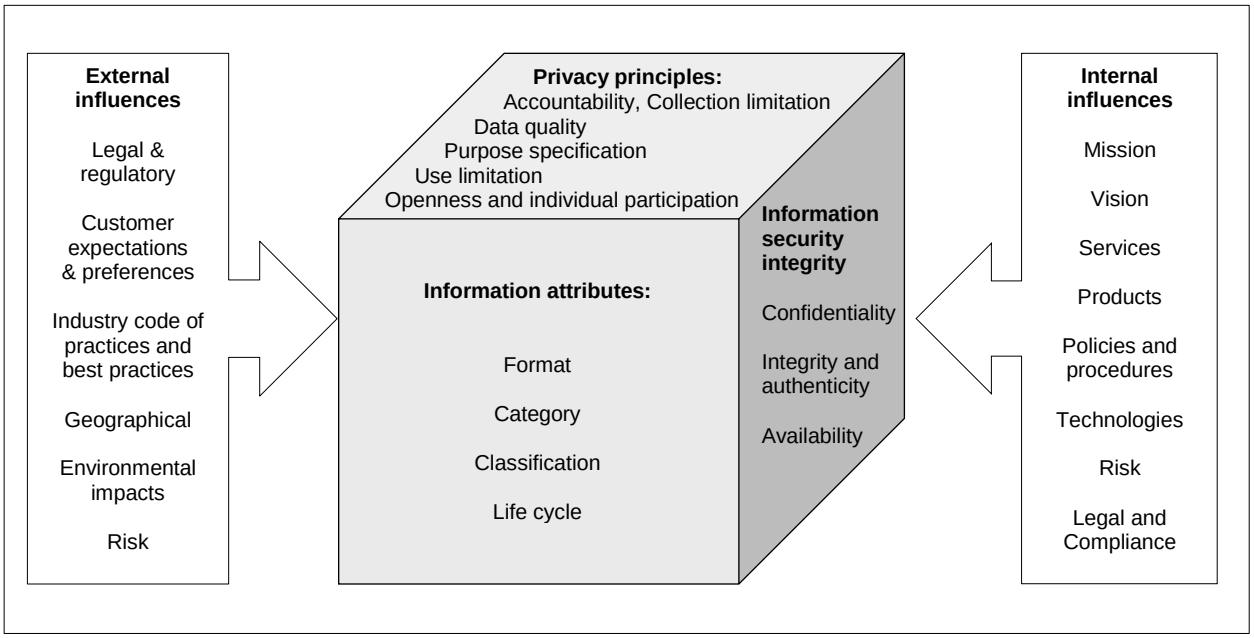
- Openness: There should be a general policy of openness about developments, practices and policies with respect to personal information processed by the responsible party. Internal privacy policies and external privacy statements (e.g. privacy policy on a website) are examples of how the responsible party established openness of personal information processing to its customers.

- Individual participation: Individuals should have the right to request whether a responsible party holds their personal information and to request access thereto as well as where necessary, the correction, destruction or deletion of his, her or its personal information. This implies that organisations should have an access request process in place and also align it to other relevant legislation, for instance the Promotion of Access to Information Act 2 of 2000 of South Africa.

- Accountability: A responsible party should be accountable for complying with the principles and measures which give effect to the principles stated above. Typical measures that should be implemented are governance structures with an information or privacy officer role, a privacy programme, auditing and monitoring, awareness programmes, and risk assessments, to mention but a few.

The OECD Guidelines have been endorsed by the U.S. Federal Trade Commission and is regarded as the most widely adopted of the frameworks for fair information practices according to Swire and Berman (2007). As such, the OECD Guidelines are used as input to define attributes of information that relate to privacy principles. Of the eight OECD Guidelines, only security safeguards are depicted as an attribute of information in the model portrayed in figure 2. The seven remainder guidelines can be added as information attributes from a privacy perspective. Figure 3 lists the information attributes to represent a comprehensive view of information from an information security and information privacy perspective.

Figure 3: Information attributes from an information security and privacy perspectives



Information security and information privacy is closely aligned. Privacy of information is often referred to as the "what" and information security as the "how". Information security is possible without privacy, but privacy of information cannot be achieved without information security (Swire & Bermann, 2007).

Information privacy or data privacy is defined as the rights and obligations of individuals and organisations with respect to the collection, use, retention, and disclosure of personal information (GAPP 2006). King III relates data privacy to the, "relationship between the collection and dissemination of data, technology, the public expectations of privacy, and the legal and political issues surrounding them." The United States refers to the term "privacy" and the European Union refers to "data protection", which is used when referring to privacy-related laws and regulations (Swire & Bermann 2007). For the purpose of this research the term information privacy is used.

Information security and information privacy focuses on the confidentiality of information through the limitation principles of privacy. Similarly, integrity is required by the data quality principle and availability through the openness principle. Information security as such is fully integrated in the security safeguards principles of privacy.

3.4 Information security culture and information protection culture

Organisations need to ensure that their employees are aware of information security and privacy policy requirements which encapsulate regulatory requirements. Employees need to understand the risk to the information they process, implement the required controls to protect it and take accountability for their actions. A culture should be inculcated in which compliance behaviour for all sensitive and confidential information, including personal information, is evident. A culture must be established in which information is protected from risk and the privacy of the information is maintained.

Schein (1985) defines culture as "a pattern of basic assumptions – invented, discovered, or developed by a given group as it learns to cope with its problems of external adaptation and internal integration – that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems". According to Schein (1985), the core substances of corporate culture are the basic assumptions, attitudes and beliefs of employees, which relate to the nature of people and their behaviour and beliefs. Assumptions are values that become embedded and as such are almost taken for granted. These basic assumptions are non-debatable and non-confrontable (Schein 1985).

Organisational or corporate culture is expressed in collective values, norms and knowledge of organisations. Values relate to the sense that people have of what ought to be. Many values are adopted consciously and guide the actions of employees (Schein 1985). Such norms and values affect the behaviour of employees and are expressed in the form of artefacts and creations. Artefacts are the visible output of a culture, for example, the written or spoken language or the way status is demonstrated (Schein 1985).

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

By introducing the concept of privacy it becomes necessary to extend the definition of information security culture and to formulate a new definition. Considering the definition of information security culture and the concept of privacy, an "information protection culture" is defined by the researchers as, "*a culture in which the protection of information and upholding of privacy are part of the way things are done in an organisation. It is a culture in which employees illustrate attitudes, assumptions, beliefs, values and knowledge that contribute to the protection and privacy of information when processing it at any point in time in the information life cycle, resulting in ethical and compliant behaviour."*

An information security culture can be present in an organisation without an information protection culture, however, the opposite is not true. In order to foster a strong information protection culture one would require a strong information security culture in the same way that privacy is dependent on information security. An organisation that has a strong information protection culture will be evident in employees processing information in a secure manner and upholding privacy principles when processing personal information.

4. Assessing an information protection culture

Compliance with privacy legislation and organisational privacy policies are achieved through various means. The regulatory environment and risks to information continuously evolves and hence most organisations implement a privacy program that is continuously monitored and audited (Herath 2011). Initially most privacy programs commence with a gap assessment to establish the existing gaps in processes, procedures and controls. Since information security is embedded in privacy, the information technology environment is also included in the scope of such gap assessments. Once action plans are defined for identified gaps, monitoring functions are initiated to track progress. Continuous monitoring of compliance with policies and procedures are

conducted together with quality control exercises. Privacy compliance can also be incorporated in internal and external audits. Privacy impact assessments (PIA) can be utilised to identify privacy risks in information systems and the early stages of system development and project planning (Herath 2011). Privacy self-assessments are often conducted by business units to improve their privacy systems and compliance. Various templates exist that organisations can refer to when conducting self-assessments, such as the Generally Accepted Privacy Principles (GAPP 2006), the Privacy Impact Assessment Framework of the European Commission (PIAF 2012), the Privacy Impact Assessment Guidelines of the Information Commissioner's Office of the United Kingdom (ICO 2014) or the maturity model developed by the Canadian Institute of Chartered Accountants (Chartered Accountants of Canada 2011). Employee awareness levels can also be assessed through online training tests.

The aforementioned assessment approaches focus on compliance with legislation and minimising risks to the processing of personal information from a process and technology perspective. The human factor is dealt with through awareness programmes and assessing knowledge of employees in respect of acceptable usage requirements for information. In the previous section we introduced the concept of an information protection culture. A holistic view of privacy compliance from a process, technology and people perspective can be obtained if the traditional methods are supplemented with an assessment of the information protection culture in the organisation. An information protection culture assessment can be of benefit to assess the current culture and identify actions to improve and monitor it over time. This will allow organisations to instil a culture whereby the workforce adopts the privacy principles as the way things are done in the organisation when processing information, including personal information.

4.1 Using ISCA to assess an information protection culture

The Information Security Culture Assessment (ISCA) (Da Veiga et al. 2007; Da Veiga & Eloff 2010) assesses the perception and attitude of employees regarding specific dimensions which are a hybrid of organisational culture and information security concepts in order to assess an information security culture. It was found that traditional privacy assessment questionnaires could not be used to assess an information protection culture as the questions were not phrased to assess the attitude and perceptions of employees. The ISCA questions are specifically designed to assess attitude and perception in line with an information security culture framework. One can argue that the ISCA instrument can be used to an extent to assess an information protection culture when taking into account that information security is part of information privacy. A prerequisite would be that the information attributes, as identified in figure 3, are assessed by ISCA to ensure that it incorporates the information attributes from an information security and information privacy perspective.

The ISCA dimensions or constructs were customised and adapted for industry purposes. For the purpose of the case study the ISCA was further customised and a privacy construct was added. The information attributes in line with the OECD Guidelines were not incorporated as such in the ISCA, as the privacy dimension that was added, was aligned to the organisation's specific requirements. It gauges the perception of certain privacy principles in line with the organisation's privacy policy such as online privacy, privacy preferences and privacy in the context of social media.

The privacy dimension added to ISCA is thus not comprehensive in terms of the privacy information attributes, but can assess it to some extent. Table 1 outlines the information attributes

identified in this research that will be important when assessing an information protection culture. An abbreviation is included in brackets. The second column is used to determine whether ISCA, as deployed in the case study organisation, deals with the specific information attributes identified for the purpose of this research. The last column provides comments relating to the whether the attribute is addressed by ISCA.

Table 1: ISCA evaluated against the information attributes

Information attributes	**ISCA**	**Comments**
1. All information formats (FO)	Yes	All information formats are assessed by ISCA
2. Category to include personal information (CA)	Yes	All information that is classified as confidential or sensitive is assessed by ISACA. Personal information is regarded as confidential. This is typically included in a definition of the term "information" upfront in the ISCA questionnaire.
3. Information life cycle to include all phases (LC)	Yes	Information in all of the life cycles is assessed by ISCA.
4. Information classification to include confidential information (IC)	Yes	All information that is classified as confidential or sensitive is assessed by ISACA.
5. Confidentiality (CO)	Yes	The perception regarding confidentiality is assessed in ISCA. Statements regarding information security controls, e.g. clear desk policy, taking information off-site, password usage, third party disclosure, etc.
6. Integrity and authenticity (IA)	Yes	The perception regarding integrity is assessed in ISCA. Statements regarding completeness and accuracy of information are included.
7. Availability (AV)	Yes	The perception regarding availability is assessed in ISCA. Statements regarding business continuity are included.
8. Accountability (AC)	Yes	The perception regarding individual and organisational accountability and responsibility towards the protection of information is assessed.
9. Collection limitation (CL)	Yes	There a statement pertaining to collection limitation.
10. Data quality (DQ)	Yes	The perception regarding data quality is assessed in ISCA. Statements about completeness and accuracy of information are included.
11. Purpose specification (PS)	No	There are no statements pertaining to purpose specification.
12. Use limitation (UL)	Yes	The perception regarding use limitation is

		assessed in ISCA. The perception regarding limitation of sharing of sensitive information is included.
13. Security safeguards (SS)	Yes	Perceptions regarding security safeguards are assessed in ISCA Multiple statements are included focussing on security controls and the management of information security.
14. Openness (0P)	No	There are no statements pertaining to openness.
15. Individual participation (IP)	No	There are no statements pertaining to individual participation.

Table 1 indicates that 12 of the 15 information attributes relating to information security and information privacy are covered by the ISCA questionnaire used in the case study. Although the privacy dimension's statements are not aligned to the OECD privacy principles (information privacy attributes) it does incorporate most of it.

An information security culture is necessary when instilling an information protection culture. Thus, in assessing an information protection culture one would also need to assess an information security culture. From a theoretical perspective one can conclude that the ISCA can be expanded to deal with all the information privacy attributes. As part of this study a validity and reliability analysis was conducted on the data derived from the case study that could be used to further improve the questionnaire from a theoretical and statistical perspective. The validity and reliability analysis can also provide insight into construct validity of the ISCA dimensions and constructs (Da Veiga et al. 2007; Da Veiga & Eloff 2010) which were customised for the purpose of the case study.

5. Research methodology

The research study was conducted by means of a case study using a quantitative assessment. The organisation chosen for the case study is a global financial institution operating across 12 countries. The organisation employed 8 220 employees in 2013. The organisation processes financial data on a global basis which is of a sensitive nature and which must be kept confidential from unauthorised parties. In addition, the organisation has to comply with a number of legislative and industry requirements when processing the financial data of organisations and individuals. From a privacy perspective, the data privacy laws in the Australia, Hong Kong, Ireland, Jersey, Mauritius, the UK, the USA and South Africa apply to the organisation. The organisation has established information security policies from an information technology (IT), end user and privacy perspective. The governance of information security across the organisation is affected through country's Information Security Officer (ISO) who reports to the Group ISO.

5.1 Sample

The data collection was conducted over a period of four years, with the first assessment done in 2010 and the last in 2013. The data of the 2013 assessment is used in this research as it incorporates the final changes to the questionnaire as required by the participating organisation. A four week period was used for each of the two assessments to allow employees time to respond to

the questionnaire. The ISCA questionnaire was sent out electronically to all employees. This method is referred to as convenience sampling (Brewerton & Millward 2001). In both assessments, an adequate number of responses were obtained for the overall data analysis:

- 2013 survey: 367 responses were required and 2 159 responses were obtained
- 2010 survey: 364 responses were required and 2 320 responses were obtained

This means that the findings could be generalised across the group. The sample size calculation used was based on a marginal error of 5% and confidence level of 95%, to ascertain the findings across the organisation (Krejcie & Morgan, 1970). In 2013, a 38,7% response rate was obtained and 28% in 2010. Non-managerial employees represented almost two thirds of the responses in 2013, with the rest being managers. Less than 3% of the respondents were made up of executives.

5.2 The measurement instrument

The ISCA questionnaire supplemented with the privacy construct was deployed in the case study organisation. The questionnaire constructs are as following:

1. Information asset management: Assesses users' perceptions of the protection of information assets
2. Information security management: Assesses management's perceptions of information security management
3. Change management: Assesses the perceptions about change and the willingness of users to change in order to protect information
4. User management: Assesses user awareness and training with regard to the requirements to protect information
5. Information security policy: Assesses whether users understand the information security policy and whether communication thereof was successful
6. Information security programme: Assesses the effectiveness of investing in information security resources
7. Trust: Assesses the perceptions of users regarding the safekeeping of private information and their trust in the communications of the organisation
8. Information security leadership: Assesses users' perceptions of information security governance (eg monitoring) to minimise risks to information
9. Training and awareness: Assesses employees' perception of additional needs for information security training
10. Privacy perception: Assesses employees' perception of privacy principles

The fifty five culture questions are measured, using a 5-point Likert scale (Strongly disagree, Disagree, Unsure, Agree, Strongly agree). The scale indicates the respondents' degree of agreement or disagreement with the statements made in each case (Dillon, Madden & Firtle 1993**)**. The option "unsure" was used as it was preferred by the organisation participating. Biographical questions were included to segment the data into twelve countries, thirteen business units, and three job levels. The biographical questions are measured using a single response scale. The objective of the biographical segmentation was to identify any areas of development across the organisation on which to focus efforts and interventions to improve the information protection culture. Knowledge questions were also added to assess information security awareness levels and to correlate it with the culture statements. A yes/no scale was used for the knowledge questions.

6. Case study findings

Table 2 outlines the ISCA dimensions with the corresponding mean and percentage agreement for each dimension for the two assessments. The mean represents the overall mean for a respective dimension comprising a number of statements. The arrows indicate whether the results for a dimension improved (arrow pointing upwards), remained the same (arrow being horizontal) or declined (arrow pointing down wards) from the previous year's assessment. A cut-off point of the mean of 4,00 was deemed acceptable for the assessment, given the importance of information security and information privacy (Da Veiga & Martins 2014).

Table 2: ISCA dimension means for 2013 and 2010

Dimensions	**Mean/% Agreement 2013 N = 2 159**	**Mean/% Agreement 2010 N = 2 320**
Information asset management	4,30, 91,2% ↑	4,22, 88,9%
Information security policies	4,15, 82,5% ↑	4,08, 80,5%
Change management	4,14, 86,1% ↑	4,09, 84,7%
User management	4,14, 85,8% ↑	4,08, 83,4%
Information security programme	4,05, 80,55 ↑	3,96, 76,8%
Information security Leadership	4,03, 82,1% ↑	3,88, 76,1%
Information security management	3,96, 80,1% ↓	4,14 90,6%
Trust	3,95, 76,8% ↑	3,88, 74,8%
Training and awareness	3,08, 43,0% ↑	3,02, 39,9%
Privacy perception	3,67, 65,4% ↑	3,56, 61,5%

The mean for all dimensions improved from the 2010 to the 2013 survey, except for the information security management dimension. A possible explanation could be the restructuring in the organisation that occurred during the four years, which might have affected the management of information security across the business units. The developmental areas identified in the 2010 assessment were identified and specific action plans were implemented. One of the key action plans that the organisation implemented related to focussed training and awareness for employees. This contributed to the positive influence on the means. It was further supported by a statistical significant difference between employees who attended the training (4,15 for the mean) as opposed to those who did not (3,96 for the mean) (Da Veiga & Martins 2014).

From a privacy perspective, most employees indicated that the organisation has clear directives on how to protect sensitive/confidential client and employee information. Employees also perceived the limitation of the collection and sharing of sensitive, personal information as important.

Less than half of the respondents indicated that the organisation's client data was complete and accurate, with only half of the respondents who believed their colleagues ensure that client information is protected when taken off site. Both these views improved significantly from the 2010 to the 2013 survey.

Interestingly, only 27% of employees believe that access to social networking sites will enhance their work activities; however the percentage increased significantly since 2010, with 24,6%. This could indicate that over the four years employees started to integrate social media more in their work. Employees seemed to have different views on whether they would be comfortable if their employer monitors what they post on social media – 52% were comfortable with 40% that disagreed and rest being neutral. Seventy four per cent of employees indicated that it is acceptable to them if employees were disciplined if they posted inappropriate comments about the organisation on social networking sites. This is supported by their perception that it is important to limit the collection and sharing of sensitive, personal information (92%).

The most critical developmental finding relating to privacy resulted in the question whether third parties that have access to personal information preserve the confidentiality of the information. Only 47,9% of employees believed that third parties of the organisation preserved the confidentiality of client information that they process on behalf of the organisation. Data privacy laws for example, the Protection of Personal Information Act 4 of 2013 (PoPI 2013) requires that responsible parties ensure that third parties maintain security safeguards as required by the act and that the relationship is governed by a written contract. There are implications from an information security as well as information privacy perspective if third parties do not preserve the confidentiality of personal information processed on behalf of the organisation. If the confidentiality of client or employee information is not maintained by third parties of an organisation it could result in unauthorised access to the data and/or disclosure. This could lead to possible identity theft, fraud, money-laundering, data breaches, regulator fines and ultimately impact on the organisation's reputation in the event of a breach.

A feedback report of the findings and recommendations were given to the organisation for both surveys which allowed them to take corrective action where indicated. The improvement in the means of the 2013 survey illustrated the impact of the action plans and how it ultimately leads to the improvement of the overall information security culture and as such the information protection culture.

7. Validity analysis

To determine the factorability and the sampling adequacy of the ISCA, the Kaiser-Meyer-Olkin measure of sampling adequacy and Bartlett's test of sphericity were first conducted. Both the indicators provided adequate scores. Principal axis factoring (PCA) was postulated and the factor matrix obtained was rotated to a simple structure by means of a varimax rotation (Brewerton & Millward 2001, Howell 1995). The scree plot was used to determine the number of factors that should be included in the measurement. From the use of the Kaiser criterion, it emerged that nine

factors could be extracted, explaining 54,3% of the total variance based on the cumulative percentage of Eigen values. Statements with a value greater than 0,3 were retained and could be regarded as meaningful to be included in a dimension (Hintze 1995). Table 3 indicates the factors with the number of statements grouped into the newly identified factors (dimensions) as well as the statement numbers.

Table 3: Results of the first factor analysis

Factors	**Number of statements/items**	**Statements**
Factor 1	20	49, 55, 50, 54, 62, 35, 61, 58, 57, 28, 60, 22, 56, 24, 66, 64, 42, 21, 47, 32
Factor 2	13	44, 43, 30, 36, 45, 29, 34, 38, 46, 53, 19, 27, 52
Factor 3	5	26, 23, 39, 31, 33
Factor 4	6	48, 63, 40, 20, 59, 41,
Factor 5	5	69, 65, 70, 67, 68
Factor 6	2	71, 72
Factor 7	3	25, 37, 51

A second-phase factor analysis was conducted to establish whether the items in factor 1 could be further divided into sub-dimensions. The analysis indicated that the items could be grouped into two new dimensions as outlined in table 4.

Table 4: Second phase factor analysis – Factor 1

Factors	**Number of statements/items**	**Statements**
Factor 1	12	54, 60, 64, 57, 49, 62, 61, 66, 50, 56, 42, 47
Factor 2	8	21, 28, 24, 22, 55, 35, 32, 58

8. Reliability analysis

The Cronbach alpha was calculated to determine the reliability of each factor (Church & Waclawski 1998).

Table 5 indicates the six final factors (dimensions) of ISCA with the corresponding Cronbach alpha and dimension description. The results indicate that the Cronbach alpha for factor 4 can be improved to 0,930 if statements 23 and 39 are omitted. These statements, however, relate to the measurement of the effectiveness of information security communication efforts. Owing to the importance of assessing the communication efforts, the statements were included. The Cronbach alpha for all six factors was above 0,7, which was deemed acceptable as a minimum value (Brewerton & Millward 2001). The six factors identified can be used as the dimensions (constructs) of the validated information protection culture assessment (IPCA) questionnaire. The columns to the right of table 5 indicate which of the information assets identified in table 1 are dealt with in each of the IPCA dimensions.

The information privacy attributes are covered to a lesser extent in IPCA as opposed to the information security attributes. Four of the information privacy attributes are contained in Factor

6 namely, collection limitation (CL), data quality (DQ), usage limitation (UL) and security safeguards (SS). Accountability (AC) is included in Factor 1 up to Factor 4.

Statements are required in IPCA for purpose specification (PS), openness (OP) and individual (IP) participation as these information attributes are omitted from IPCA. In order to measure a construct effectively a minimum of three statements are required per construct (Hair et al 2010). It is thus concluded that the IPCA can be further improved by adding at least three statements for each of the information privacy attributes. This will contribute to the content validity of the IPCA and allow for a second validity and reliability analysis. Any additional questions should reflect the perception and attitude of employees towards the privacy principles as opposed to questions that verify controls, which are phrased to test the design of control or operating effectiveness of controls typically used in compliance, gap assessments or audits. The IPCA should also allow for scalability in terms of regulatory requirements between different jurisdictions and thus assess the principles of privacy as opposed to regulatory requirements of a specific jurisdiction. Regulatory requirements of a jurisdiction can though be covered in the knowledge section of the IPCA questionnaire.

Table 5: Information protection culture dimensions

				Information attributes														
Factor	**Cronbach alpha**	**IPCA dimension**	**Description**	FO	CA	LC	IC	CO	IA	AV	AC	CL	DQ	PS	UL	SS	OP	IP
Factor 1	0,887	Information security commitment	The perception on the commitment from an organisational, divisional and employee perspective regarding the protection of information and implementation of information security controls.	✓	✓	✓	✓	✓	✓	✓	✓					✓		
Factor 2	0,766	Management buy-in	The perception on management buy-in towards information security and the importance attached to the concept by senior managers and executives. The concept of management adherence to the information security policy is also established.	✓	✓	✓	✓	✓	✓	✓	✓					✓		
Factor 3	0,878	Information security necessity and importance	Information security necessity is established by focusing on specific concepts such as people, time, money and the impact of changes.	✓	✓	✓	✓	✓	✓	✓	✓					✓		
Factor 4	0,798	Information security policy effectiveness	The effectiveness of the information security policy and the communication thereof is established.	✓	✓	✓	✓	✓	✓	✓	✓					✓		
Factor 5	0,803	Information security accountability	Individual accountability to compliance and the requirements for information security training.	✓	✓	✓	✓	✓	✓	✓						✓		
Factor 6	0,764	Information usage perception	The perception on information security and privacy usage requirements.	✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓		

9. Discussion

The first aim of the paper was to introduce the concept of an information protection culture and to explain the difference between an information security culture and information protection culture (research question). This culture encapsulates the concept of an information security culture together with privacy principles. Having a strong information protection culture will aid in minimising the risk posed to the protection of information, which includes personal information, from a human perspective. This aids the researchers in answering the first research question, "What is the difference between an information security culture and an information protection culture?"

An information protection culture is inclusive of an information security culture whereas an information security culture can exist without an information protection culture. Most organisations process personal information about their employees, clients and/or juristic persons. This necessitates a culture whereby all information is protected at all times to mitigate risk and hence the focus on information security. By processing personal information organisations also have to meet regulatory compliance requirements and customer expectations. The CIA of information security does not incorporate all the privacy principles such as openness and purpose specification. Organisations could experience a gap in protecting personal information they process if only information security is considered and a culture is embedded focussing on information security without incorporating privacy of information.

The attributes of information defined in this research can aid organisations in understanding the various aspects that must be considered to protect information from a holistic perspective which will aid in instilling an information protection culture as oppose to only an information security culture.

The second aim and research question was to establish if the ISCA instrument can be utilised to assess an information protection culture. The ISCA can be used to assess an information protection culture as an information protection culture encompasses an information security culture. However, the ISCA constructs were improved with the validity analysis and new constructs are proposed. The new constructs provide input for an information protection culture assessment (IPCA) instrument. The defined information attributes (table 1) provide insight to identify what needs to be assessed from an information privacy perspective. Three of the information attributes are not incorporated in the IPCA and hence statements must be defined to be in line with privacy principles, such as the OECD privacy guidelines. This will contribute to the content validity of the questionnaire. Adding the additional statements to the IPCA will necessitate that the validity and reliability test be conducted again to derive a final IPCA questionnaire. To further enhance the IPCA an information protection culture framework should also be defined to facilitate the content validity of the IPCA and to aid with implementation in organisations.

10. Conclusion

Information privacy and information security are two interrelated concepts that consider the protection of information. Both must be considered when dealing with information risk from a human behaviour perspective as most organisations process personal information together with other types of confidential and sensitive information. Employees must process confidential

information in all formats and categories through its life cycle in a secure manner. Their behaviour can be directed through aspects such as policies, compliance requirements, training and awareness, monitoring as well as fostering a strong information protection culture. An information protection culture assessment (IPCA) can be conducted to establish what the perceptions of employees are regarding the protection of information from an information security and information privacy perspective. The output of an IPCA can be used to direct employee behaviour and focus initiatives on specific content or biographical groups in the organisation such as specific job levels of departments.

This research aimed at defining what an information protection culture is with the objective of facilitating the development of an information protection culture assessment questionnaire. This was achieved by evaluating an existing information security culture assessment (ISCA) questionnaire against the information attributes defined in the research. It was found that the ISCA can be used to assess an information protection culture. The ISCA was deployed in a case study organisation and certain information privacy concepts were included in the assessment. The case study data was used to conduct a factor and reliability assessment. It was found that the IPCA is valid and reliable, but that additional constructs should be defined and included in the IPCA to facilitate the content validity of the questionnaire.

Future research will aim to develop the information privacy constructs of the IPCA by means of an information protection culture framework that can provide input to the statements of the IPCA questionnaire. The researchers aim to then conduct a second validity and reliability assessment to finalise the IPCA questionnaire. One of the limitations of the current empirical data is that only one international organisation's data was used for the validation of the IPCA. It would further enhance the validity and reliability of the IPCA if future studies can include organisations from various industries to confirm the validity and reliability across organisations and industries.

11. References

Charandtered Accountants of Canada (2011) *AICPA/CICA Privacy maturity model*. Available from: http://www.cica.ca/resources-and-member-benefits/privacy-resources-for-firms-and-organizations/docs/item48094.pdf [Accessed 14 July 2014].

APEC, *vide* Asia Pacific Economic Cooperation (2005) *Asia Pacific Economic Cooperation (APEC) privacy framework.* Retrieved from www.apec.org/.../ECSG/05_ecsg_privacyframewk.ashx [Accessed 14 July 2014].

Brewerton, P. & Millward, L. (2001) *Organizational research methods*. London: Sage.

Bruening, P.J., Sotto, L.J., Abrams, M.E. and Cate, F.H. (2008) *Strategic information management.* .Bureau of National Affairs, Inc.

Church, A.H. & Waclawski, J. (1998) *Organizational surveys: a seven step approach*. San Francisco: Jossey-Bass.

Da Veiga, A. and Eloff, J.H.P. (2007) An information security governance framework. *Information Systems Management*, 24(4),361–372.

Da Veiga, A. and Eloff, J.H.P. (2010) A framework and assessment instrument for information security culture. *Computers and Security*, (29),196–207.

Da Veiga, A. and Martins, N. (2014) Information security culture: a comparative analysis of four assessments. *Proceedings of the 8th European Conference on IS Management and Evaluation*, 8,49–57.

Da Veiga, A., Martins, N. and Eloff J.H.P. (2007) Information security culture – validation of an assessment instrument. *Southern African Business Review*, 11(1),147–166.

Dillon W.R., Madden J.T., Firtle, N.H. Essentials of marketing research. Boston: IRWIN;1993.

European Commission (EC) (2014) Reform of Data Protection Legislation. Available from: http://ec.europa.eu/justice/data-protection/ [Accessed 25 November 2014]

EU Data Directive 95/48/EC (1995) Available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. [Accessed 14 July 2014].

Generally Accepted Privacy Principles (GAPP) (2006) *A global privacy framework, privacy*. Available from: http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/GAPP_BUS_%200909.pdf [Accessed 14 July 2014].

Gou K.H. (2013) Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, (32), 242–251.

Greenfield, G. (2014) Sheherezade and the 101 data privacy laws: origins, significance and global trajectories. *Journal of Law, Information and Science*. 23(1), 1–48.

Hair J. F. Jr., Black W. C., Babin B. J., and Anderson R. E. (2010) Multivariate data analysis: A global perspective (7th ed.) New York: Pearson.

Herath, K.M. (2011) *Building a privacy program: a practitioner's guide.*Portsmouth: International Association of Privacy Professionals.

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

Hintze, J.L. (1995) Number cruncher statistical systems (Version 5.03 5/90)[Computer Software]. Kaysville, UT: NCSS.

Howell, D.C. (2011) Fundamental statistics for the behavioral sciences, 3rd International Standards Organisation. Available from: http://www.iso.ch

IBM SPSS Statistics (2011) (*Version 21.0 for Microsoft Windows platform*)[Computer Software]. Chicago, IL: SPSS Inc.

Information Commissioner's Office (ICO) (2014) Conducting Privacy Impact Assessments Code of Practice, Version: 1.0. Available from: http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/pia-code-of-practice-final-draft.pdf [Accessed 25 November 2014]

Infosecurity Europe Industry Report (2014) Available from: Infosecurity_Europe_2014_FULL_REPORT_From_business_barrier_to_business_enabler [Accessed 14 July 2014].

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

Johnson, M.E. and Goetz, E. (2007) Embedding information security into the organization. *IEEE Security & Privacy*, (5),16–24.

King Code of Governance for South Africa (2009) Institute of Directors Southern Africa. Available from: http://www.iodsa.co.za/?kingIII [Accessed 9 October 2014].

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

Liginlal, D., Sim, I. and Khansa, L. (2009) How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management, *Computers and Security*, (28), 215–228.

OECD Privacy Principles (1980) Organisation of Economic Cooperation and Development. Available from: http://oecdprivacy.org/. [Accessed 1 September 2014].

Padayachee, K. (2012) Taxonomy of compliant information security behaviour. *Computers and Security*, (1), 673-680.

PCI DSS Requirements and Security Assessment Procedures (Version 2.0.) (2010) PCI Security Standards Council LLC. Available from: https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf [Accessed 1 August 2014].

PricewaterhouseCoopers (PwC) (2014) The Global State of Information Security Survey. Available from: http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml [Accessed 20 February 2014].

Privacy Impact Assessment Framework (PIAF) (2012) Recommendations for a privacy impact assessment framework for the European Union. Available from [http://piafproject.eu/ref/PIAF_D3_final.pdf]

Ponemon. Cost of Data Breach Study: Global Analysis Benchmark research sponsored by Symantec; 2013, Available from: http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-2013. [Accessed 20 February 2014].

Promotion of Access to Information Act (PAIA) 2 of 2002. (2002) Available from: http://www.acts.co.za/ [Accessed 20 September 2014].

Protection of Personal Information Act (POPI) 4 of 2013. (2013) Available from: http://www.acts.co.za [Accessed 20 September 2014].

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

Swire, P.P. and Berman, S. (2007) *Information privacy, official reference for the certified information privacy professional*. Portsmouth: IAPP.

The Standard of Good Practice for Information Security (SOGP). (2007) Information Security Forum.

UN Universal Declaration of Human Rights. (1948) Available from: http://www.un.org/en/documents/udhr/. [Accessed 20 March 2014].

Zurich, Data security: A growing liability threat fact sheet. (2009) Available from: http://www.zurichna.com/NR/rdonlyres/23D619DB-AC59-42FF-9589-C0D6B160BE11/0/DOCold2DataSecurity082609.pdf [Accessed 20 March 2014].