Comparing the information security culture of employees who had read the information security policy and those who had not

Illustrated through an empirical study

Received 18 December 2015
Revised 18 December 2015
Accepted 9 March 2016

Adéle Da Veiga
School of Computing, University of South Africa (Unisa), Johannesburg, South Africa

Abstract

Purpose – This study aims, firstly, to determine what influence the information security policy has on the information security culture by comparing the culture of employees who read the policy to those who do not, and, secondly, whether a stronger information security culture is embedded over time if more employees have read the information security policy.

Design/methodology/approach – An empirical study is conducted at four intervals over eight years across 12 countries using a validated information security culture assessment (ISCA) questionnaire.

Findings – The overall information security culture average scores as well as individual statements for all four survey assessments were significantly more positive for employees who had read the information security policy compared with employees who had not. The overall information security culture also improved from one assessment to the next.

Research limitations/implications – The information security culture should be measured and benchmarked over time to monitor change and identify and prioritise actions to improve the information security culture. If employees read the information security policy, it has a positive influence on the information security culture of an organisation.

Practical implications – Organisations should ensure that employees have read the information security policy to aid in minimising the human risk, related errors and incidents and, ultimately, to instil a stronger information security culture with a higher level of compliant behaviour.

Originality/value – This research confirms theoretical research indicating that the information security policy could influence the information security culture positively. It provides novel and statistical evidence illustrating that if employees read the information security policy, they have a stronger information security culture and that the culture can be improved through targeted interventions using an ISCA.

Keywords Assessment, Information security, Policy, Culture, Influence, Factors

Paper type Research paper

Introduction

"The success of an information resources protection program depends on the policy generated, and on the attitude of management towards securing information on

Information & Computer Security
Vol. 24 No. 2, 2016
pp. 139-151

2056-4961
DOI 10.1108/ICS-12-2015-0048

automated systems." This statement was included in a special publication of the National Institute of Standards and Technology (NIST) in 1989 (Whitman and Mattord, 2014). Technology has evolved significantly since then, with an expectation that by 2020, there will be 50 billion internet-connected devices, including fixed communications, mobile communications, computers, consumer electronic devices, medical devices, industrial devices and automotive devices (Ponemone Institute, 2015). One of the top priorities of organisations in managing information and minimising risks is still to have a written information security policy (PwC, 2014). This policy provides the formal direction and intent of management for the protection of information in the organisation. It outlines the framework for setting control objectives and controls to be implemented to mitigate risk to information (ISO/IEC 27001, 2013).

The information security policy is implemented through a combination of people, processes and technology controls. From a people perspective, the policy directs the manner in which employees process information and establishes a baseline from which ethical decisions are made when dealing with organisational information. The policy influences the way in which employees interact with information assets and ultimately directs their behaviour to be compliant with legislative, regulatory and contractual requirements.

The information security policy is a critical success factor to establish a strong information security culture in an organisation. Employees' knowledge and perception of information security policy rules and procedures influence information security behaviour and potentially the information security culture (ISF, 2000; Box and Pottas, 2013). The more aware employees are of the information security policy and procedures, the more positive their attitude becomes towards it, resulting in risk-averse behaviour (Parsons *et al.*, 2014). If a strong information security culture is present, it will improve the information security (Bulgurcu *et al.*, 2010) and enable an environment in which information is protected from a people, process and technology perspective.

Aim of the paper

In an organisation where management aims to institutionalise the information security policy, there will be a group of employees who have been exposed to or trained in the information security policy contents, as well as a group of employees who must still be exposed or trained. This could be due to a phased approach of implementing training and awareness, staff turnover, changes or updates to the policies that must be communicated or employees being on leave or sick at the time of the training, to mention a few reasons. One could argue that the group of employees who have read the information security policy would have a shared understanding of the organisation's common values to protect information and that their information security culture might be different from that of employees who have not read the policy.

This research study aims to determine whether there is a difference between the information security culture of employees who have read the information security policy and those who have not. A contribution of this research is to provide empirical evidence to confirm literature perspectives indicating that the information security policy could influence the information security culture positively. Another is to provide empirical evidence that a strong information security culture can be inculcated over time through the awareness and understanding of the information security policy. In support of the aforementioned, the following research questions are posed:

RQ1. Do employees who have read the information security policy have a stronger information security culture compared to those who have not?

RQ2. Does the overall information security culture become stronger if more employees have read the information security policy?

The remainder of the paper is structured as follows: background to the influence of information security policies on an information security culture is provided. This is followed by outlining the development of an information security culture. Next, the research methodology and results of the information security culture survey conducted in the case study organisation are presented. The discussions and limitations of the research study are discussed, followed by the conclusion.

Background

There are various studies that aim to establish how to influence employees to comply with information security policies. It is generally concluded that one of the internal influences on policy compliance is the organisational culture. The organisational culture influences the effective implementation of the information security policy, as it impacts the perception employees have about information (Knapp *et al.*, 2009). As part of this theory, awareness and training are regarded as two of the processes required to govern the implementation of the information security policy. Von Solms and Von Solms (2004) suggest that policies can in turn define the organisational culture using continuous education and communication. Thomson *et al.* (2006) propose the information security shared tacit espoused values (MISSTEV) model. The aim of this model is to instil behaviour that is in line with the information security policy and that could lead to the cultivation of an information security culture.

Apart from awareness and training, there are various other factors that also influence perceptions of employees' compliance with information security policies. Herath and Rao (2009) identify three facts that influence policy compliance, namely, threat perceptions about the severity of breaches, organisational commitment and social influences and resource availability. Cross-cultural differences can also influence ethical decision-making (Hoffstede, 1980; Jackson, 2000), the normative belief system of employees (Pahnila *et al.*, 2007), the perception of senior management commitment and users' personal values and standards of conduct (Leach, 2003), the use of rewards to motivate compliance (Bulgurcu *et al.*, 2010) and the readability and understandability of the policy language (Goucher, 2012), which are all factors that could potentially influence employees' compliance with information security policies.

Padayachee (2012) proposed a taxonomy for compliant information security behaviour by considering extrinsic (e.g. regulatory requirements) and intrinsic (e.g. employee competence, their commitment, ethical values, personality, values and attitude) motivations. A crucial conclusion from Ifinedo's (2014) research is that attitude towards compliance has the greatest effect on information security policy compliance. Similarly, Siponen *et al.* (2014) argue that employees' perceived severity, vulnerability, self-efficacy, normative beliefs and attitude have a positive and significant impact on their intention to comply with information security policies and procedures. More recently, Sherif *et al.* (2015) proposed five variables that could influence information security culture, namely, information security behaviour, top management support, security education and awareness, the information security policy and information

security acceptance. Their research incorporates the role that the information security plays on culture while being part of a wider project to establish how the information security culture influences the compliance of employees towards information security requirements.

While these studies focus on factors that influence or motivate employees to comply with the information security policy, some dimensions have not yet been tested empirically. One such dimension is the influence of awareness of the information security policy on the information security culture by comparing the culture of employees who have read the policy with those who have not, within the context of an information security culture assessment (ISCA) (Da Veiga and Martins, 2015).

ISCA can be used to assess employees' attitude towards policy compliance and information security culture aspects. The outcome can be used to determine if there is a strong information security culture present in the organisation. A strong information security culture postulates that employees exhibit compliance behaviour, have coherent values towards protecting information and thus minimise the threat of the human element to information.

Development of an information security culture

To understand what impact an information security policy has on the information security culture, how such a culture develops must be understood. The development of an organisational culture can be leveraged off to ascertain how an information security 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. This culture will incorporate specific organisational behaviour (Hellriegel *et al.*, 1998).

Similarly, an information security culture develops in an organisation in the same way an organisational culture develops (Figure 1). The board is responsible for ensuring that information assets are managed effectively and should approve the organisation's information security strategy (King III, 2009). The board will delegate responsibility for implementing information security and management needs to demonstrate their commitment and buy-in. They will provide the direction and intent for the protection of

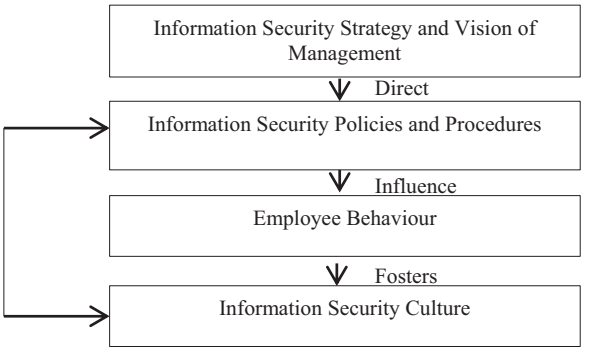

Figure 1.
Development of an information security culture

information through the information security policy. They could, for instance, 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, employees will respond to the policy as influenced by extrinsic and intrinsic factors. The information security culture that emerges could be conducive to the protection of information or hamper it. It is therefore crucial to assess the information security culture that has emerged and to determine whether it is in line with the initial information security strategy and vision of management.

The role of the information security policy

NIST (2010) defines an information security policy as an aggregate "of directives, regulations, rules, and practices that prescribes how an organisation manages, protects, and distributes information". The information security policy sets out the organisation's approach to information security and provides a framework for setting control objectives and controls, including the structure of risk assessment and risk management (ISO/IEC 27001, 2013). An information security policy is regarded as a best practice by ISO27002 (2013). According to the standard, it serves "to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations".

The information security policy is only effective in directing employee behaviour to protect information if employees are aware of the policy and understand how to implement it. Best practice standards such as ISO/IEC 27001 (2013), The standard of good practice for information security (2007) and the Information Security Forum (ISF, 2000) emphasise that awareness and training programmes should form part of the information security programme to communicate policy requirements to employees. It is essential that the information security policy be published in a location where employees can access it. It should be communicated to all employees, including contractors, temporary staff, trainees as well as third parties. ISO/IEC 27001 (2013) states:

> All employees of the organisation and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function.

The ISCA can aid management in conducting a reality check and taking corrective action to redirect the information security culture. Statistical analysis of the ISCA data can provide insight into the factors that have to be included to influence employees' perception of and attitude towards the information security policy and ultimately contribute to a stronger information security culture.

Research methodology

This research study comprised a quantitative study in which a survey was conducted at four intervals over eight years in an international organization, as described in the following sections.

Research philosophy

A positivism philosophy is used to assess the information security culture using a structured methodology with quantitative methods, including statistical analysis

(Saunders *et al.*, 2009). The objective of positivist research is to obtain research results that are reliable, consistent, unbiased and replicable through other research studies to represent reality (De Villiers, 2012). The survey approach is thus used to conduct the ISCA being generally used to assess attitudes and opinions by systematically gathering data from the population for a specific purpose (Kraut, 1996).

Measuring instrument

To establish the impact of an information security policy on the information security culture, a validated information security culture instrument (questionnaire) must be used to measure the level of information security culture, as well as to monitor the impact of the interventions. For the purpose of this study, the ISCA questionnaire is used. This questionnaire is a validated information security culture questionnaire that has been adapted for industry purposes, of which the reliability is between 0.764 and 0.877 (Da Veiga and Martins, 2015).

The ISCA has nine dimensions (constructs), one of which specifically relates to the information security policy. In total, ISCA has 44 information security culture-related statements that are used to assess information security culture. Seven of these statements relate to the information security policy. The information security culture statements are rated on a five-point Likert scale (Strongly Disagree, Disagree, Unsure, Agree, Strongly Agree) to assess the employees' degree of agreement or disagreement with the statement (Dillon *et al.*, 1993).

In total, 15 yes/no questions are included in ISCA to gauge the information security awareness of certain concepts and to draw correlations with the information security culture statements. The ISCA's yes/no statements were customised for the case study organisation and three additional yes/no statements pertaining to the information security policy were added. This resulted in a total of 18 information security awareness statements in the ISCA questionnaire.

The ISCA also includes biographical questions (e.g. business units, countries and job levels) to segment the data for intervention and comparison purposes.

Case study organisation

The case study organisation operates across 12 countries and has one overarching Group Information Security Policy. To determine the effectiveness of the information security programme in the organisation, various methods were used by the Group ISO, e.g. the implementation of technology and process safeguards, governance, risk assessments, monitoring, auditing and country self-assessments.

There was also a need to determine whether there is a positive information security culture in the organisation and how employees perceive information security requirements that they have to conform with. As such, ISCA was incorporated in the information security programme.

Sample

A cross-sectional design was used for the study where data were collected on more than one case, but at a single point in time across a number of variables (Bryman, 2008). The ISCA was deployed in the case study organisation in 2006 to measure the level of information security culture present in the organisation. A number of interventions were identified as a result of the 2006 ISCA, some of which related to the information security policy. After the interventions were implemented, a second ISCA was needed to

determine if they had a positive impact on the information security culture. This cycle was repeated four times, as depicted in Table I.

The organisation employed 3,927 employees in 2006, which increased to 8,220 employees in 2014. The convenience sampling method (Brewerton and Milward 2002) was used, whereby the survey was distributed electronically to all employees in the organisation across all 12 countries.

Each of the ISCAs was conducted over a period of four to five weeks to give employees time to respond to the survey. The required sample was calculated for each ISCA occasion based on a marginal error of 5 per cent and a confidence level of 95 per cent, to ascertain the findings across the organisation (Krejcie and Morgan, 1970). For each of the ISCA occasions, an adequate number of responses were obtained in line with the 95 per cent confidence level.

Statistical analysis

Survey software, namely, Survey Tracker (2014), was used to distribute the electronic questionnaire and to conduct the statistical analysis. The SPSS version 22 (2013) software package was used to conduct *t*-tests to determine the significant differences between the results of the group of employees who had read the information security policy compared with those who had not (Brewerton and Millward, 2002). Regression analysis was further used to determine the most important focuses of each year (Da Veiga and Martins, 2015).

The overall information security culture rating or score was determined (i.e. the average of all the items across the constructs) for the organisation as a whole and for the biographical groups such as the countries, departments and job levels. The lowest and highest items were identified per biographical group to identify developmental areas and action plans for the organisation.

The information security policy-related statements in the ISCA that were below the accepted cut-off of 4.00 for the mean were identified and specific action plans defined to address them. As the information security culture level was also monitored, the average scores for the ISCA dimensions were tracked and compared as well as any constructs that were identified as developmental areas.

Results

Overall information security culture

The information security culture mean improved from one assessment to the next, with the most positive results in 2013, as illustrated in Table II. This mean represents the information security culture level in the organisation, as assessed using the nine constructs of ISCA. The mean for the 2013 ISCA was the most positive when compared with the mean of the other years, indicating that the information security culture

	ISCA 1	ISCA 2	ISCA 3	ISCA 4
Year	2006	2007	2010	2013
Number of employees	3,927	5285	7014	8,220
Sample required	351	351	364	367
Responses obtained	1,941	1,571	2,320	2,159

Table I. ISCAs and interventions over eight years

improved from 2006 to 2013. The means of the four ISCA occasions illustrate the value of conducting the ISCA over a period to monitor the impact of the interventions and change in information security culture.

In 2010, a decline in the results was observed, which could have related to the business restructuring that occurred during that period. However, the results in 2013 improved to above the cut-off of 4 for the mean.

The results indicate that the information security culture that was fostered became more positive over time. One reason for the improvement is attributed to training and awareness initiatives (Da Veiga and Martins, 2014). The second could be related to the implementation of the action plans and an increasing number of employees who have read the information security policy.

After the 2010 ISCA, a focused awareness programme regarding the information security policy was implemented. This constituted monthly e-mails explaining specific requirements in the information security policy. A brochure was also compiled with a summary of the policy in easily understandable language. The location of the policy and the importance of reading it were emphasised in the communications.

These activities might have positively influenced the overall information security culture average score from 2010 to 2013. However, to examine the actual impact of the awareness and communication interventions of the information security policy on the information security culture, further comparison analysis was conducted, as discussed in the next paragraph.

More positive overall information security culture for employees who had read the policy compared to those who had not

To further explore if having read the information security policy results in a more positive or stronger information security culture, the data of all the information security culture constructs measured were segmented between the group of employees who had read the policy and those who had not. This was possible because a question was added in the ISCA questionnaire where employees had to indicate whether they had read the policy or not.

The overall information security culture mean was calculated for each of the two groups and compared. An important finding is that the overall information security culture mean of the employees who had read the policy (4.10) in 2013 was higher compared with those who had not (3.94).

Table III exhibits the overall information security culture in percentage for the group of employees who had read the policy compared to those who had not. For each year that the ISCA was conducted (i.e. 2006, 2007, 2010 and 2013), the information security culture percentage is more positive for the group who had read the policy than the group who

Table II. Overall information security culture overall averages

ISCA occasion	Actual responses	Overall information security culture mean	Overall information security culture in (%)
ISCA 4 – 2013	2,159	4.10	83.6
ISCA 3 – 2010	1,320	3.76	75.7
ISCA 2 – 2007	1,571	4.00	81.7
ISCA 1 – 2006	1,941	3.89	75.7

had not. (It is important to note that the percentage in Table III indicates the overall information security culture and not the frequency of employees who have read the policy).

The information security culture is thus more positive, as measured through ISCA, for the group of employees who had read the policy compared to the group of employee who had not read the policy. The information security culture score therefore indicates that reading the information security policy has a positive impact on the information security culture of employees.

Significant differences of individual statements for employees who had read the policy compared to those who had not

The positive influence of an information security policy on the information security culture was further illustrated in the significant differences of individual statements in the ISCA of the employees who had read the policy compared with those who had not. The results of the *t*-tests indicated that all 44 statements in the ISCA were significantly more positive for employees who had read the policy compared with those who had not.

Employees who had read the information security policy had an improved understanding of it. They also believed that the policy was practical and applicable to their working environment during the execution of their daily tasks. They were significantly more positive that management and colleagues complied with the policy. For all the abovementioned concepts, they were significantly more positive compared with employees who had not read the policy.

In a strong information security culture, fewer information security incidents would be expected. This is confirmed in the data in that fewer employees who had read the information security policy shared their passwords (89.8 per cent) compared with those who had not read it (85.1 per cent). Another example is that more employees who had read the policy protected data when taking it offsite (54.8 per cent) compared with employees who had not read it (45.3 per cent). Similarly, 74.2 per cent of the employees who had read the policy took care when talking about confidential information in public places compared with 69.6 per cent of the employees who had not read it.

Increase in numbers of those who had read the policy compared to those who had not

The frequency of employees who had read the information security policy increased from 1,057 employees in 2006 to 1,381 employees in 2013. The awareness and communication interventions could have contributed towards motivating employees to read the information security policy. More employees (70.3 per cent) who had read the information security policy knew where to get a copy of it compared with those who had not (46.8 per cent) for the 2013 data.

Interestingly, a total of 96.9 per cent of the employees knew that the organisation had an information security policy. A total of 35.9 per cent of the employees had still not read the policy and 30 per cent did not know from where to get a copy of it. Further awareness

Table III. Information security culture for read and not read policy

Data segmentation	Overall information security culture in %			
	2013 (%)	2010 (%)	2007 (%)	2006 (%)
Group that read policy	83.6	79.6	85.6	82.0
Group that did not read policy	76.6	69.5	75.0	68.1

and communication interventions for specific biographical groups need to be conducted to improve this. An advantage of the ISCA is that the job levels, countries and business units can be identified with low frequencies of employees who had read the information security policy to be targeted through initiatives.

Discussion and limitations

This research study makes a contribution to the information security discipline and specifically in relation to the human threat to information protection. It strongly supports the notion that reading the information security policy has a positive influence on the information security culture. This is confirmed through the data derived from an ISCA that was conducted at four intervals over eight years across 12 countries.

The data analysis showed that the group of employees who had read the information security policy had a stronger information security culture based on the more positive overall mean of ISCA and the individual statements that were significantly more positive than the group who had not read the policy. This provides empirical evidence that employees who read the information security policy have a stronger information security culture compared with those who had not, thereby answering *RQ1*.

RQ2, relating to whether the overall information security culture becomes stronger if more employees have read the information security policy, is answered by considering the overall information security culture average score, which improved for each of the ISCAs. This score can be seen as a description of the dominant information security culture, representing the perception of the majority of the employees. The employees who have not read the policy represent a subculture with a lower information security culture score (Martins and Martins, 2016). A subculture represents a certain group of employees who share common values related to their work environment or geographical area, for instance, which is not necessarily similar to the dominant culture that represents the majority of the employees (Martins and Martins, 2016).

An information security policy plays a critical role in directing an information security culture. The implication for organisations is that an information security policy is imperative, but if employees have not read it or understood it, it will not be effective in directing their behaviour, influencing their attitude towards policy compliance or fostering a strong information security culture. At least one in every three organisations still does not have written information security- or privacy-related policies in place and up to 24 per cent do not have an acceptable usage policy in place (Protiviti, 2014). The 2015 Information Security Breaches Survey (ISBS, 2015) indicates that "72 per cent of companies where the security policy was poorly understood had staff related breaches". This not only introduces risk to the protection of information, but could also have legal implications and ultimately inculcate an information security culture that is not beneficial towards the protection of information.

The value of ISCA has been illustrated in this research in that the information security culture is influenced positively by addressing the developmental areas identified in the assessment. Information security policy awareness was one critical developmental area. By having an increased number of employees who have read the information security policy, the overall culture is influenced positively.

As discussed earlier, there are numerous factors that influence employees' willingness to comply with the information security policy. Similarly, there are also various factors that influence the development of a strong information security culture.

A limitation of this research study is that external factors that could potentially influence the information security culture were not considered, for example national culture.

Conclusion

The results of this study provide statistical evidence that the information security culture of employees who had read the information security policy is significantly more positive when compared with employees who had not. Reading the information security policy contributes to influencing the information security culture positively. Over time, a stronger information security culture is developed. The dominant information security culture, which represents the common perception of the majority of the employees, became stronger over time, as indicated through the ISCA scores of the employees who read the policy, as well as the improvement of the overall ISCA scores. In turn, the information security culture of the group of employees who had not read the policy, representing a subculture, also became stronger, although it was overall lower when compared with the group of employees who had read the information security policy.

Awareness of an information security policy contributes in fostering an information security culture. In such an environment, fewer information security incidents from a human perspective and more risk-adverse behaviour would be expected. This study emphasises the value of awareness initiatives regarding the information security policy and serves as a motivation to prioritise having an adequate policy and communicating it to employees. This will help as a motivation to eliminate the gap between the percentage of organisations that do not have awareness initiatives in place regarding their information security policy and those that do.

Although this study focused only on the influence of information security policies, further research will examine the influence of other factors on the development of an information security culture, such as leadership and trust. The influence of national culture will also be explored in future work to develop an ISCA tool that considers factorial invariance across countries. Further analysis will also be conducted to investigate other possible subcultures of information security across the organisation and how to positively influence the culture by focusing on subcultures.

References

Box, D. and Pottas, D. (2013), "Improving information security behaviour in the healthcare context", *Procedia Technology*, Vol. 9 No. 2013, pp. 1093-1103.

Brewerton, P. and Millward, L. (2002), *Organizational Research Methods*, Sage Publications, London.

Bryman, A. (2008), *Social Research Methods*, 4th ed., Oxford University Press, New York, NY.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Q*, Vol. 34 No. 3, pp. 523-548.

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*, Vol. 8 No. 2014, pp. 49-57.

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

De Villiers, M.R. (2012), "Models for interpretive information systems research, part 1: is research, action research, grounded theory – a meta – study and examples", in Mora M., Gelman O., Steenkamp A. and Raisinghani M.S. (Eds), *Research Methodologies, Innovations and Philosophies in Software Systems Engineering and Information Systems*, IGI Global, Hershey.

Dillon, W.R., Madden, J.T. and Firtle, NH (1993), *Essentials of Marketing Research*, IRWIN, Boston.

Goucher, K.R.W. (2012), "Health service employees and information security policies: an uneasy partnership?", *Information Management & Computer Security*, Vol. 20 No. 4, pp. 296-311.

Hellriegel, D., Slocum, J.W. Jr and Woodman, R.W. (1998), *Organizational behavior*, 8th edn., South-Western College Publishing, PA.

Herath, T. and Rao, H.R. (2009), "Protection motivation and deterrence: a framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18 No. 2009, pp. 106-125.

Hoffstede, G. (1980), *Culture's Consequences: International Differences in Work-related Values*, Sage Publications, Beverley Hills.

Ifinedo, P. (2014), "Understanding information systems security policy compliance: an integration of the theory of planned behaviour and the protection motivation theory", *Computers & Security*, Vol. 31 No. 2011, pp. 83-95.

Information Security Breaches Survey (ISBS) (2015), "PricewaterhouseCoopers", available at: www.pwc.co.uk/assets/pdf/2015-isbs-executive-summary-02.pdf (accessed 4 December 2015).

Information Security Forum (ISF) (2000), *Information Security Culture – A Preliminary Investigation*, Information Security Forum, London.

ISO/IEC 27002 (2013), *Information Technology – Security Techniques – Code of Practice for Information Security Management*, ISO/IEC 27002.

Jackson, T. (2000), "Management ethics and corporate policy: a cross cultural comparison", *Journal Management Studies*, Vol. 37 No. 2000, pp. 349-369.

King Code of Governance for South Africa (King III) (2009), "Institute of directors Southern Africa", available at: www.iodsa.co.za/?kingIII (accessed 9 October 2014).

Knapp, K.J., Morris, R.F., Marshall, T.E. and Byrd, T.A. (2009), "Information security policy: an organizational-level process model", *Computers & Security*, Vol. 28 No. 2009, pp. 493-508.

Kraut, A.I. (1996), *Organizational Surveys*, Jossey-Bass Publishers, San Francisco, CA.

Krejcie, R.V. and Morgan, D.W. (1970), "Determining sample size for research activities", *Educational and Psychological Measurement*, Vol. 30 No. 1970, pp. 607-610.

Leach, J. (2003), "Improving user security behavior", *Computers & Security*, Vol. 22 No. 8, pp. 685-692.

Martins, E. and Martins, N. (2016), "Organisational culture", in Robbins, S.P., Odendaal, A. and Roodt, G. (Eds), *Organisational Behaviour*, 3rd ed., Pearson Education, Cape Town, pp. 606-641.

National Institute of Standards and Technology (NIST) (2010), "NIST special publication 800-37: guide for applying the risk management framework to federal information systems", available at: www.nist.gov/manuscript-publication-search.cfm?pub_id=916094 (accessed 4 December 2015).

Padayachee, K. (2012), "Taxonomy of compliant information security behavior", *Computers & Security*, Vol. 31 No. 2012, pp. 673-680.

Pahnila, S., Siponen, M. and Mahmood, A. (2007), "Employees' behaviour towards IS security policy compliance", in Sprague, R.H. Jr (Ed.), *40th Hawaii International Conference on System Sciences (HICSS 07)*, *IEEE Computer Society, Washington, DC*.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014), "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)", *Computers & Security*, Vol. 42 No. 2014, pp. 165-176.

Ponemone Institute (2015), "Global cyber impact report", available at: www.aon.com/risk-services/thought-leadership/2015-global-cyber-impact-report.jsp (accessed 22 September 2015).

PricewaterhouseCoopers (PwC) (2014), "The global state of information security survey", available at: www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml (accessed 10 December 2014).

Protiviti (2014), "IT security and privacy survey", available at: www.protiviti.com/itsecuritysurvey, (accessed 11 December 2014).

Saunders, M., Lewis, P. and Thornhill, A. (2009), *Research Methods for Business Students*, 5th ed., Pearson.

Sherif, E., Furnell, S. and Clarke, N. (2015), "An identification of variables influencing the establishment of information security culture", in Tryfonas, T. and Askoxylakis, I. (Eds), *The Human-Computer Interaction (HCI) Conference – Human Aspects of Information Security, Privacy and Trust (HAS)*, HAS 2015, LNCS 9190, pp. 436-448.

Siponen, M., Mahmood, A. and Pahnila, S. (2014), "Employees' adherence to information security policies: an exploratory field study", *Information & Management*, Vol. 51 No. 201, pp. 217-224.

SPSS version 22. (2013), *IBM Software Group, ATTN: Licensing, 200 W*, Madison St., Chicago, IL.

Survey Tracker (2014), Training Technologies Inc., available at: www.surveytracker.com/ (accessed 7 June 2014).

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

Thomson, K., Van Solms, R. and Louw, L. (2006), "Cultivating an organisational information security culture", *Computer Fraud and Security*, Vol. 2006 No. 10, pp. 7-11.

Von Solms, R. and Von Solms, B. (2004), "From policies to culture", *Computers & Security*, Vol. 23 No. 2004, pp. 275-279.

Whitman, M.E. and Mattord, H.J. (2014), *Management of Information Security*, 4th edn., Cengage, Stamford.

About the author

Adéle Da Veiga holds a PhD in Information Technology. She is employed at the University of South Africa in the School of Computing. Her research projects relate to information security culture and privacy with related empirical studies in industry. She has published journal papers in *Computers & Security, Computer Law & Security Review, Journal of Governance and Regulation, Information Systems Management; Southern African Business Review* and *South African Computing Journal*. She is also a rated researcher under the National Research Foundation. Prior to her academic career, she was employed for 13 years in the industry, where she specialised in information security, information governance, audit, risk management and privacy. She holds a Certified Information Systems Auditor (CISA) and a Certified Information Privacy Technologist (CIPT) certification. Adéle Da Veiga can be contacted at: dveiga@unisa.ac.za