An Information Security Training and Awareness Approach (ISTAAP) to Instil an Information Security-Positive Culture

A. Da Veiga

College of Science, Engineering and Technology, School of Computing, University of South Africa, P.O. Box 392, UNISA 0003, South Africa
e-mail: dveiga@unisa.ac.za

Abstract

This paper proposes a unique information security training and awareness approach (ISTAAP) that can be used to instil an information security-positive culture which will assist in addressing the risk that human behaviour poses to the protection of information. An information security culture assessment tool is used as the critical diagnostic instrument to assess the information security culture within the context of ISTAAP. A case study is discussed where the ISTAAP was deployed. This provided empirical data to illustrate the value of ISTAAP to direct employee behaviour through focused training and awareness based on the outcome of the information security culture assessment data.

Keywords

Information security culture, awareness, training, approach, survey, measure, human, people, behaviour

1. Introduction

Information security training and awareness are two of the most effective offsets to mitigate the human risk posed to information security (Parsons *et al*., 2014). Current and former employees in organisations are still regarded as a risk to the protection of information and are often the cause of information security incidents (Schlienger and Teufel, 2005, Ashenden, 2008, Thomson *et al*., 2006, Herath and Rao, 2009, Kraemer *et al*., 2009, Herold, 2011, Furnell and Clarke, 2012, Furnell and Rajendran, 2012, Padayachee, 2012, Crossler *et al*., 2013, Flores *et al*., 2014, PwC, 2014). Research indicates that up to a third of incidents are caused by employees (Ponemon, 2013). This could be as a result of deliberate attacks, error or negligence of employees. Consequently, organisations need to prioritise employee information security training and awareness to close the gap from an employee perspective.

However, information security training and awareness are regarded as a challenge for many organisations (PwC, 2014) for a number of reasons. Some of the reasons relate to the constant change in information technology, the numerous devices in which information is processed, the wide distribution of locations where information is accessed and stored and the heightened regulatory environment for handling and processing information (Herold, 2011). These aspects result in organisational policy

changes that employees need to constantly be made aware of and trained in to ensure compliance and to minimise the risk to information. In addition, the general awareness of employees, their computer literacy levels and the organisational budget could be a hindrance to the effectiveness of information security awareness programmes (Shaw *et al*., 2009).

Information security training is essential in organisations to embed compliance behaviour in line with the information security policy requirements and to yield lasting behaviour changes (ISF, 2000). Whilst training is deployed in organisations to increase knowledge on a certain subject or trait or to change behaviour, it also improves skill and can change employee attitude (Berry & Houston, 1993). Effective training and awareness both result in behavioural change in organisations and are critical in embedding information security principles at employee level. Information security awareness initiatives are often conducted in conjunction with information security training to build and sustain an information security-positive culture (ISF, 2002). Cobit for Information Security (2012) emphasises the importance of creating information security awareness at organisational and individual level. By stimulating effective information security training and awareness at all levels in an organisation, a positive information security culture can be promoted to enhance protection of information, minimise risk and contribute to compliance (Hassan and Ismaila, 2012, Da Veiga and Martins, 2015).

The aim of this research study is to define an approach that can be deployed to focus information security training and awareness efforts. This, in turn, contributes to instil an information security-positive culture. In order to achieve the research aims, the information security training and awareness approach (ISTAAP) is proposed and was deployed in an international organisation to establish whether it yielded positive results as part of an empirical study. This research study aimed at complementing the body of literature on information security training and awareness by empirically testing the theoretical, proposed ISTAAP model to establish its impact on information security culture.

2. Background

2.1. Reasons for stimulating information security training and awareness

Information security training help to minimise the risk of employee behaviour by deliberately focusing on a set of learning experiences to increase information security knowledge (Berry & Houston, 1993), such as what confidential information is, what the risks are to information and what employees should do to protect information. The information security training can further help improve employee skills when, for instance, using encryption, selecting a strong password or including information security controls in system design. The attitude of employees towards the implementation of information security controls can also be influenced positively. In time, this becomes the way things are done and inculcates a positive information security culture (Da Veiga and Eloff, 2010).

Information security training and awareness can be used to ensure that information security policy requirements become part of the knowledge base of employees, enabling them to meet policy requirements (Thomson *et al*., 2006). Information security training is also deployed to orientate new employees through induction training, which includes an overview of policies and procedures of the organisation (Byars and Rue, 1997).

The Organisation for Economic Co-operation and Development (OECD, 2002) emphasises the need to develop a strong information security culture through various factors, two of which are training and awareness. The ISO/IEC 27002 (2013) also emphasises the importance of information security training and awareness. The objective of this training and awareness should be to move from an information security-negative or neutral culture to an information security-positive culture. This will contribute to sustainable change in employee attitude as well as their behaviour towards information security. Attitudes and beliefs together with basic assumptions are the core substances of corporate culture and as such also of an information security culture (Schein, 1985). It is therefore critical that the approach to information security training and awareness integrate the concept of information security culture.

2.2. Existing approaches for implementing information security training and awareness

Information security training and awareness have to be managed as part of the information security programme in a structured and organised manner. In many instances information security awareness campaigns are conducted on an ad hoc basis, for instance communication e-mails are sent out and posters are placed in key locations. Organisations also use computer-based training modules and newsletters, include information security sessions in induction training and hand out promotional items, such as mouse pads with information security information on them (Albrechtsen & Hofden, 2010). Engaging in these activities could create the perception that "all is well" and that management can tick the box. This creates the expectation that employees are aware of the information security policy requirements and will exhibit compliance behaviour.

Organisations cannot illustrate due diligence by merely indicating that they have conducted training and awareness without evaluating the effectiveness of the actions implemented. The effectiveness of training and awareness is often evident in the culture of the organisation when certain behaviour becomes the accepted norm. Employees might use unprotected memory sticks for back up or save confidential client information in an unprotected cloud environment. These behaviours could result in potential information security incidents and data breaches if the information is accidently lost, exposed, accessed or changed without authorisation or used inappropriately.

The effectiveness of awareness and training is also evident in the number of existing metrics in an organisation, such as the number of information security and privacy

incidents, network downtime as a result of malicious code, customer complaints, findings in audit and risk reports, inappropriate authorisations for transactions, regulatory fines or the number of lost information assets such as laptops and portable storage devices (Herold, 2011).

Organisations need to utilise a method to evaluate the effectiveness of information security awareness and training programmes. Parsons *et al.* (2014) developed the human aspects of information security questionnaire (HAIS-Q) to evaluate the information security health of an organisation by assessing employee knowledge, attitude and behaviour in relation to information security. It does not, however, use a validated information security culture questionnaire based on information security culture constructs to direct and target employee behaviour of certain stakeholder groups. Herold (2011) introduced a comprehensive approach to identify current awareness and training needs, create a roadmap and develop, deliver and evaluate the training. Various evaluation methods are included ranging from checklists and surveys to computer-based training assessments, the output of which is used to tailor future awareness and training topics and delivery methods. This method does not incorporate a validated and reliable questionnaire to assess the impact of awareness on the information security culture, nor to assess whether the efforts contributed to a security-positive culture, but rather focuses on improving the awareness levels in the organisation.

Other researchers have also defined approaches to implementing information security awareness and training (ISF, 2002, Zakaria and Gani, 2003, Schlienger and Teufel, 2005, Thompson *et al.,* 2006, Power and Forte, 2006, Kruger and Kearney, 2006, Kritzinger and Smith 2008, Albrechtsen and Hovden, 2010). None of the current approaches propose an information security awareness and training approach that is holistic comprising formal phases that extend to assessing the effectiveness of the awareness and training within the context of an information security culture using a validated assessment instrument. Such an approach would allow the impact of training and awareness on the information security culture to be determined through valid and reliable results, and would also enable continuous monitoring of changes and the implementation of corrective actions to ensure that an information security-positive culture is sustained.

As such, the following research questions were defined:

- Does the ISTAAP serve as an effective approach to implement information security training and awareness initiatives whereby success can be measured in the context of an information security culture?
- Is the ISTAAP effective to focus information security training and awareness initiatives?

3. Information security training and awareness approach (ISTAAP)

The ISTAAP is proposed in Figure 1. It is a holistic approach focusing on inculcating an information security-positive culture in an organisation to aid in mitigating the risk of the human element in the protection of information. ISTAAP is a unique approach in the sense that it incorporates an information security culture assessment as a core element to direct training and awareness. ISTAAP consists of four distinct phases which are implemented on a cyclical basis. Each phase comprises of a number activities that are conducted in response to the ISCA that is conducted in the evaluate effectiveness phase.

Evaluate Effectiveness (EE): Prior to developing training and awareness, it is essential to conduct a needs analysis (Berry and Houston, 1993, Byars and Rue, 1997, Herold, 2011). During this phase the information security culture level is assessed using the information security culture assessment (ISCA) (Da Veiga and Martins, 2015) as an initial needs assessment and to benchmark future assessments. The ISCA questionnaire comprises of nine constructs, each with items that have to be answered on a Likert scale.

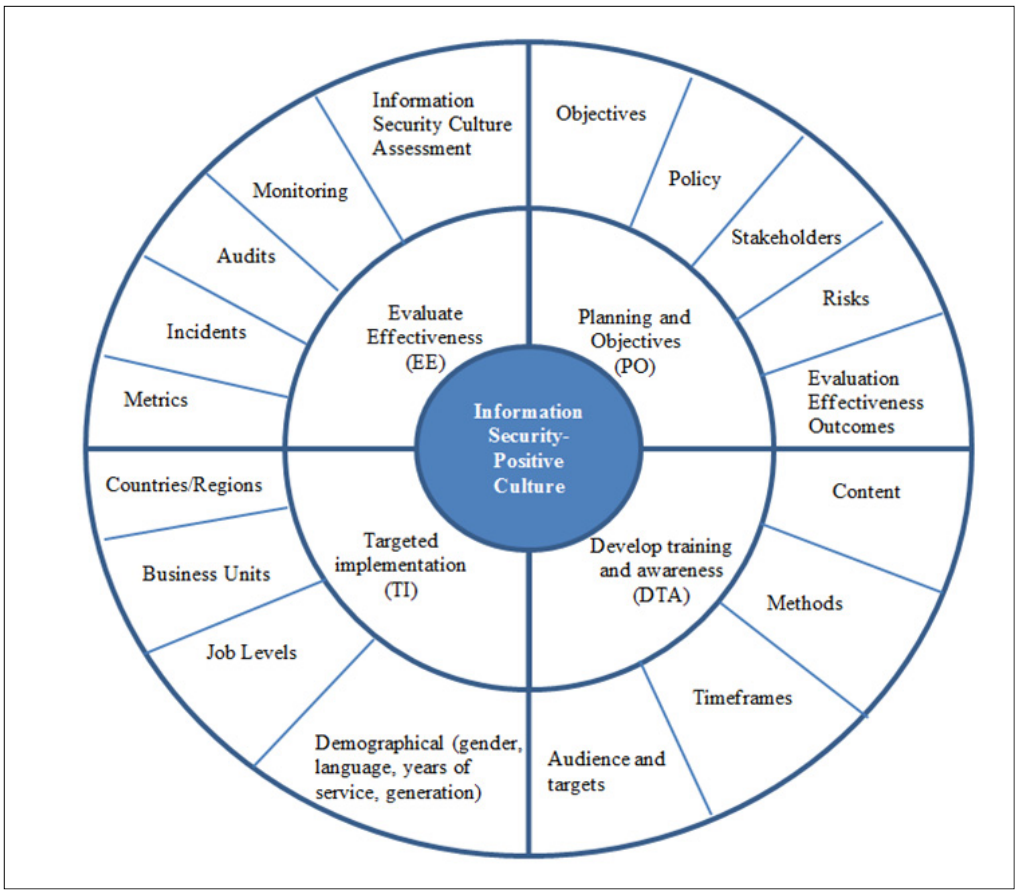

Figure 1: Information security awareness and culture model (ISTAAP)

The ISCA assessment is conducted in the form of an electronic survey, which is distributed to all employees in the organisation to complete. Focus groups are also used to confirm the results of the ISCA. Empirical data is derived from the ISCA to understand the level of information security culture in the organisation, the required content of training and awareness and the stakeholders to prioritise based on their information security-negative (or low) culture.

The overall information security culture rating or score is 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, job levels, generation groups or ethnic groups. The lowest and highest items are identified per biographical group to identify focus areas for training and awareness activities. Further statistical analysis is conducted to identify recommendations for improvement which is discussed under the case study findings.

As ISCA has been validated through statistical methods, it provides valid and reliable results over time to facilitate employee attitude and related behaviour change to inculcate an information security-positive culture (Da Veiga and Martins 2015).

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

Planning and Objectives (PO): The information security training and awareness objectives are derived from the business and information security strategy, but also based on the information security policy and regulatory requirements. The impact and value of ISTAAP are derived by tailoring the objectives and planning according to the outcomes of the evaluation of the effectiveness of the information security training and awareness as derived from ISCA.

Develop Training and Awareness (DTO): There are many techniques or methods that can be used to deliver information security training. The content, delivery method and audience need to be considered. This will depend on the effectiveness evaluation outcomes, budget available and resources to develop and deliver material. A number of methods are often used in organisations for information security training, such as web-based training, discussion groups, brown bag sessions and hands-on training (ISF, 2002, Herold, 2011). Posters, desk drops, text messages, e-mails and newsletters are categorised as awareness methods to communicate information to employees (Herold, 2011). These methods are often employed as part of an awareness programme with specific activities per month.

The outcome of the ISCA is used to define what training and awareness material and content to develop. It has been found that the ISCA results often vary between the biographical groups necessitating customised training for each group pertaining to the contents. Questions regarding to the most preferred methods of communication

are included in the ISCA to identify which method to consider for each biographical group.

Targeted Implementation (TI): The ISCA results provide empirical data with the most preferred and effective training and awareness methods per stakeholder group in the organisation. Targeted training and awareness are implemented for each group, focusing on the key concepts and preferred delivery method per group based on the ISCA data. Implementation can be conducted in order of priority, starting with the most negative biographical areas in the organisation. Implementation usually spans over a few months and even up to a year.

Once the implementation phase has been rolled out a follow up ISCA is conducted, moving on to the EE phase, to establish whether the implemented actions have had a positive impact on the information security culture. A follow up ISCA also provides insight to determine whether the identified activities were successful and whether other developmental areas arose over time. Data from more than one ISCA for a specific organisation serves as successful monitoring of the culture change over a period of time.

4. Research methodology

The research methodology in this study was a quantitative research design. The ISTAAP was deployed in an international organisation to monitor the success of the information security programme, identify where to focus training and awareness initiatives and determine what to change in order to instil an information security-positive culture. The ISTAAP cycle was repeated four times from 2006 up to 2013 by deploying the ISCA on four occasions in the organisation, see Figure 2. For the purpose of this research paper the application of the ISCA in the context of ISTAAP will be the focus in the research methodology discussion.

4.1. Sample

A period of four to five weeks was defined for employees to respond to the ISCA survey for each of the EE phases. The first ISCA was conducted in 2006 with a sample of 1 941 employees, see figure 2. A year later the second ISCA was conducted with a sample of 1 571 employees.

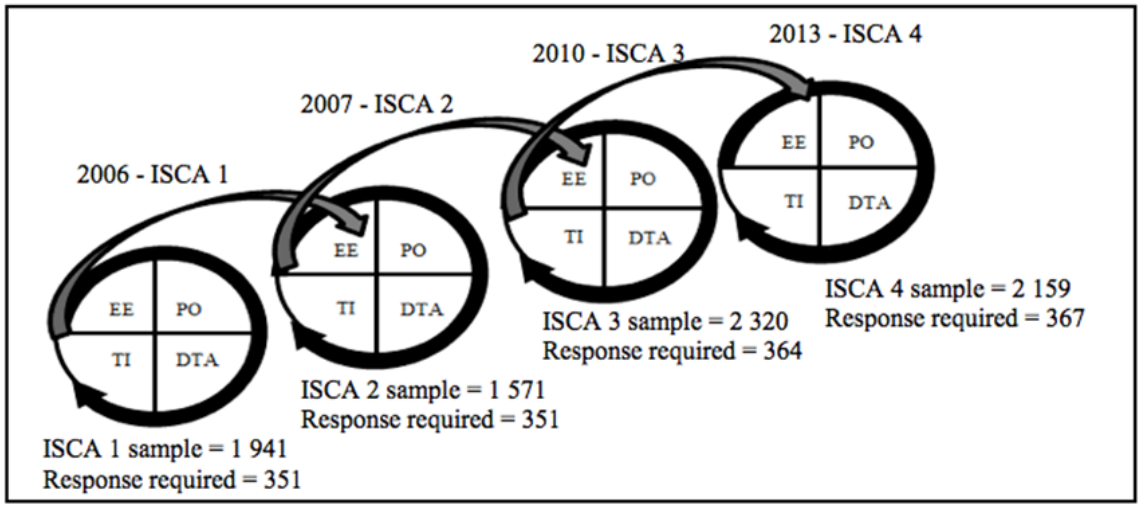

Figure 2: ISTAAP implementation cycles

The 2010 ISCA included a sample of 2 320 employees and the ISCA in 2013, a sample of 2 159 employees. The required sample was calculated for each ISCA occasion based on a marginal error of 5% and a confidence level of 95% to ascertain the findings across the organisation (Krejcie and Morgan, 1970). This is critical to ensure that the information security culture scores derived are valid for the population (i.e. organisation) and should be calculated for each implementation of ISTAAP. For each of the ISCA occasions an adequate number of responses were obtained. Corrective actions as identified in ISCA were implemented for each ISTAAP cycle.

4.2. Case study findings

The statistical analysis for each year was conducted using Survey Tracker (2015) and IBM SPSS Statistics 22 (2011). The data were analysed and the means, frequencies and frequency distribution were determined for the overall data and biographical segmentation. Anova and t-tests were used to determine the significant differences between the biographical groups in order to prioritise training and awareness initiatives. Regression analysis was further used to determine the most important focuses of each year which were used to direct the PO phase. Biographical groups with less than five responses were not included in the analysis in order to protect the respondent's confidentiality and to meet the sampling requirements. When deploying ISTAAP it is critical to conduct these statistical analyses in order to ensure that the data is interpreted correctly for management decisions.

The overall average information security culture scores improved from one assessment to the next with the most positive results in 2013. The overall mean in 2006 was 3.89, which improved to 4.10 in 2013. This data indicates that the information security culture became more positive over time. One of the reasons is related to the implementation of ISTAAP where the Group ISO implemented the recommended developmental actions as identified in each ISCA.

Figure 3 portrays the information security culture scores (% agree) for the group of employees that had received prior training and awareness compared with those that had not, as well as the overall information security culture scores. The data illustrates that the overall information security culture level improved, and thus a more positive information security culture was inculcated over time. There was a significant improvement from 2010 to 2013. The ISCA corrective actions that were implemented as part of ISTAAP contributed to this improvement.

The organisation restructured before the 2010 survey, which could be a reason for the decline in the information security culture. This illustrates that information security should also be addressed when change is instituted in the organisation to maintain the information security culture level. The improvement from the 2010 to the 2013 ISCA illustrates the positive impact of ISTAAP and the use of ISCA as the key assessment component to direct training and awareness methods to positively influence the information security culture.

Employees that had been exposed to prior training and awareness were more positive than those that had not. This illustrates the value and impact of the corrective actions as deployed in ISTAAP based on the outcomes of ISCA. It is interesting to note that the information security culture gap (level) between employees that had received prior training compared with those that did not became smaller between 2006 and 2013, see figure 3. This indicates that the information security culture level also improved for the group of employees that had not been exposed to prior training and awareness. One explanation could be that their behaviour was influenced by the group of employees that had been exposed to training and awareness and that there was overall a more positive perception of information security in the organisation.

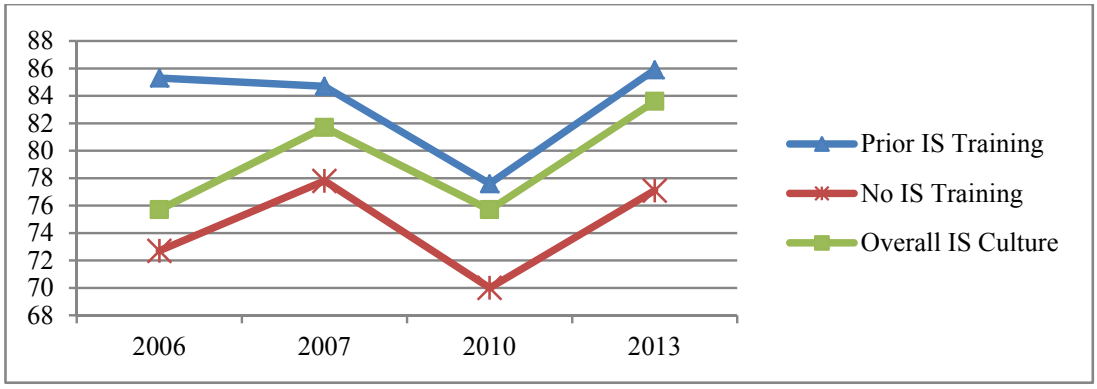

Figure 3: ISCA average scores for the four ISCAs

The statistical reports with conclusions and recommendations of ISCA were used as part of the PO phase to define the training and awareness objectives. The training and awareness content that was developed was based on the top ten most negative concepts derived from the ISCA for each biographical group.

ISCA includes a statement relating to the training and awareness preference of employees. In all four ISCAs it was found that e-mail was the most preferred method, followed by presentations and web-based training. These ISCA findings

provided input to the DTO phase in which a combined method was used to conduct training and awareness. As such, e-mails were sent on a monthly basis to all employees and group presentations were conducted in each country facilitated by the Group ISO in each instance. It is important to note that the preferred methods of communication by employees could vary between organisations.

5. Discussion and conclusion

In this research the ISTAAP is proposed as a flexible approach to tailor and focus training and awareness initiatives with the objective of inculcating an information security-positive culture. The ISCA is used as the central assessment tool in ISTAAP to determine the information security culture level. At the same time, it provides data that can be used to determine the effectiveness of training and awareness initiatives that can be leveraged off to influence the information security culture. The ISTAAP contributes to minimise the risk posed by employee behaviour as specific actions can be derived to change employee perception and ultimately employee behaviour when interacting with organisational information. The information security culture in the case study organisation became more positive over time as is evident in the data of the ISCA used within the context of ISTAAP. A more positive information security culture will result in employees displaying risk-averse behaviour, introducing less incidents, complying with policies and ultimately assisting in protecting information. ISTAAP therefore helps counter the risk posed by human behaviour by providing empirical data through ISCA to address critical constructs and biographical groups in order to positively influence the information security culture.

The first research question has been answered in that the effectiveness of ISTAAP and the success of the training and awareness is evident in the improvement of the average information security culture scores from the first assessment to the most recent one. In addition, the group of employees that had been exposed to prior information security training and awareness had a more positive information security culture compared with those that had not.

In answering the second research question, the ISTAAP was found to be effective in focusing information security training and awareness initiatives, as the empirical data can be used to identify biographical groups that are more negative compared with other groups. The data can also be used to identify the most preferred methods of communication and the critical messages to relay to each biographical group and finally the improvement can be monitored by benchmarking the data with the follow-up ISCAs.

A limitation of the research is that only the data of ISCA was considered and monitored throughout the case study. The ISTAAP can further be improved by incorporating other assessment methods and data with the ISCA data to verify the change in employee behaviour and to identify any correlations. Further research will also focus on conducting reliability and validity tests, to determine the factorial invariance across countries for the ISCA questionnaire and to establish how the impact of national culture can be incorporated in ISTAAP.

6. References

Albrechtsen, E. and Hovden, J. (2010), "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study", *Computers & Security*, Vol. 29, pp432–445.

Ashenden, D. (2008), "Information security management: A human challenge?", *Information Security Technical Report*, Vol. 13, No. 4, pp95–201.

Berry, M.L. and Houston, J.P. (1993), Psychology at work, Brown and Benchmark, Wisconsin, ISBN: 9780697246134.

Byars, L.L. and Rue, L.W. (1997), *Human resource management*, 5th edition, Irwin McGraw-Hill, Boston, ISBN: 9780256201932.

Cobit for Information Security. (2012), "ISACA", www.isaca.org, (Accessed 5 November 2014).

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013), "Future directions for behavioral information security research", *Computers & Security*, Vol. 32, pp90-101.

Da Veiga, A. and Eloff, J.H.P. (2010), "A framework and assessment instrument for information security culture", *Computers & Security*, Vol. 29, pp196–207.

Da Veiga, A. and Martins, N. (2015), "Improving the information security culture through monitoring and implementation actions illustrated through a case study", *Computers & Security*, Vol. 49, pp162-176,

Flores, W.R., Antonsen, E. and Ekstedt, M. (2014), "Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture", *Computers & Security*, Vol. 43, pp90–110.

Furnell, S. and Clarke, N. (2012), "Power to the people? The evolving recognition of human aspects of security", *Computers & Security*, Vol. 31, pp983–988.

Furnell, S. and Rajendran, A. (2012), "Understanding the influences on information security behavior", *Computer Fraud and Security*, Vol. 2012, pp12–15.

Hassan, N.H. and Ismail, Z. (2012), "A conceptual model for investigating factors influencing information security culture in healthcare environment", (ICIBSoS 2012), *Procedia - Social and Behavioral Sciences*, Vol. 65, pp1007 – 1012.

Herath, T. and Rao, H.R. (2009), "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, Vol. 47, pp154–165.

Herold, R. (2011), *Managing an information security and privacy awareness and training program*, 2nd edition, CRC Press, Boca Rotan, ISBN: 9781439815458.

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

Information Security Forum (ISF). (200), Information Security Culture – A preliminary investigation", November 2000, https://www.securityforum.org, (Accessed Feb 2009).

Information Security Forum (ISF). (2002), "Effective security awareness workshop report, April 2002", https://www.securityforum.org, (Accessed Feb 2009).

ISO/IEC 27002:2013. (2013), *Information technology – Security techniques – Code of practice for information security management*, New York.

Kraemer, S., Carayon, P. and Clem, J. (2009), "Human and organizational factors in computer and information security: Pathways to vulnerabilities", *Computers & Security*, Vol. 28, pp509–520.

Krejcie, R.V. and Morgan, D.W. (1970), "Determining sample size for research activities", *Educational and Psychological Measurement,* Vol. 30, pp607–610.

Kritzinger, E. and Smith, E. (2008)," Information security management: An information

security retrieval and awareness model for industry", Computers and Security, Vol. 27, pp124–231.

Kruger, H.A. and Kearney, W.D. (2006), "A prototype for assessing information security awareness", *Computers & Security*, Vol. 25, pp289-296.

OECD. (2002), "Guidelines for the Security of Information Systems and Networks, Towards a Culture of Security", www.oecd.org/dataoecd/16/22/15582260.pdf, (Accessed 10 June 2014).

Padayachee, K. (2012), "Taxonomy of compliant information security behavior", *Computers & Security*, Vol. 31, pp673–680.

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, pp165-176.

Ponemon Institute. (2013), "Cost of data breach study: Global analysis benchmark research sponsored by Symantec", http://www.symantec.com, (Accessed 10 June 2014).

Power, R. and Forte, D. (2006), "Case study: A bold new approach to awareness and education, and how it met an ignoble fate", *Computer Fraud and Security*, Vol. 2006, pp7-10.

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

Schein E.H. (1985), *Organizational culture and leadership*, Jossey-Bass, San Francisco, ISBN: 0875896391.

Schlienger, T. and Teufel, S. (2005), "Tool supported management of information security culture: An application to a private bank", in Sasaki, R., Okamoto, E. and Yoshiura, H., (eds) *Security and privacy in the age of ubiquitous computing*, Kluwer, Japan.

Shaw, R.S., Chen, C.C., Harris, A.L. and Huang, H., "The impact of information richness on information security awareness, training effectiveness", *Computers & Education*, Vol. 52, pp92–100.

Survey Tracker. Training Technologies Inc; (2015), https://www.surveytracker.com/. (Accessed 30 April 2015).

Thomson, K., Van Solms, R. and Louw, L. (2006), "Cultivating an organisational information security culture", *Computer Fraud and Security*, October, pp7–11.

Zakaria, O. and Gani, A. (2003), "A conceptual checklist of information security culture", in Hutchinson, B. (Ed.) *Proceedings of the 2nd European Conference on Information Warfare and Security*, MCIL, Reading, pp365-372.