Human Aspects of Information Assurance: A Questionnaire-based Quantitative Approach to Assessment

E.D. Frangopoulos[1], M.M. Eloff [2] and L.M. Venter [3]

[1] School of Computing, University of South Africa (UNISA), Pretoria, South Africa
[2] Institute for Corporate Citizenship, University of South Africa (UNISA), Pretoria, South Africa
[3] Institutional Director: Research Support and Extraordinary Professor: Computer Science and Information Systems, North-West University, Potchefstroom, South Africa
e-mail: vfrangopoulos@hol.gr; mmeloff@unisa.ac.za; lucas.venter@nwu.ac.za

Abstract

In work previously done by the authors, various human aspects of Information Assurance were identified. These comprise Social and Psychological aspects, the effects of Psycho-social risk at the workplace, the application of Influence techniques, user response to Social Engineering Methods and choices based on Economic considerations. Even though these aspects have been shown to gravely affect Information Assurance, the current level of their incorporation in the Plan-Do-Check-Act virtuous cycle of Information Security Management Systems, leaves a lot to be desired. In order to combine the findings of previous research and effectively provide quantified input that is usable in the context of an Information Security Management System (ISMS), an appropriate methodology must be introduced. This paper sets the framework and constraints for the methodology and by examining the merits and shortcomings of existing work in the field, proposes a questionnaire-based quantitative methodology that meets the set requirements. This will ultimately provide a tool for rapid, consistent and repeatable assessment of the Information Assurance level, as this is affected by the identified human aspects of Information Assurance.

Keywords

Information Assurance Assessment Tool, Questionnaire, Information Security, Quantitative vs, Qualitative, Human Aspects of Information Assurance, PDCA, ISMS, InfoSec.

1. Introduction

In the Information Security and Assurance literature it has been long established (Schneier, 2000) that the human factor is a most important component of Information Security / Assurance, perhaps even more important than the technical measures taken against threats that affect Information Assurance (IA). Even though methodologies exist that allow academics and professionals to assess the level of information-related risk in information systems in particular and information-processing organisational structures in general, it is still difficult to integrate the human factor in

the Deming (or Plan-Do-Check-Act) virtuous cycle (Deming, 1986) of an effective Information Security Management System (ISMS).

In previous work, several areas of non-technical, human aspects of IA such as Social and Psychological aspects, the effects of Psycho-social risk at the workplace, Influence techniques, Social Engineering Methods and most recently, human choices that affect IA and are based on Economic considerations, as a potential source of risk per se, were identified (Frangopoulos, Eloff & Venter, 2008; 2010; 2012; 2014).

The obvious question arising from this research is how to efficiently incorporate these vague aspects (compared to the more easily quantifiable technical issues and measures) in the IA assessment process for a given information system or an information-processing organisational structure.

Due to the human nature of these IA aspects, there is none better equipped to provide the information necessary for an assessment, than these who constitute the human element of the information system/structure themselves. To this end, information-gathering approaches that are based on focus groups, individual interviews, questionnaire distribution etc, can be directed towards the people in the organisational structure under examination, whose actions affect the IA posture of the structure.

The aim of this paper is to describe the advantages of a questionnaire-based methodology and discuss its framework and constraints, by drawing on conclusions from the authors' past work on the human aspects of IA and by benefiting from extensive work carried out on the subject of questionnaire-based methods in the field of social sciences. By examining the merits and shortcomings of existing, well-researched methodologies, the most appropriate one that meets the set requirements, will ultimately be identified.

In the discussion that follows, the foundation of such a structured methodology will be laid. At this stage, only the structure of a methodology and its governing principles will be presented, mostly based on the merits and known deficiencies of existing social science practices and adapted for the task at hand. This is a crucial first step which paves the way for future work that will examine the practical issues of how such a methodology may be applied, its scope of application and the incorporation of its results to the ISMS' virtuous PDCA cycle. This foundation work constitutes the paper's contribution to the field of the Human Aspects of Information Security and Assurance research.

2. Scope and defining qualities of the assessment methodology

In order to avoid misconceptions, it is important to clarify exactly what is expected from the proposed assessment methodology:

- Quantification in the form of percentages will be necessary.
- The methodology should be driven by and provide feedback to the ISMS effort.

- The assessment results are not necessarily expected to provide an absolute measure of any particular IA quality of the information system/structure but should be used to initially establish a baseline, while subsequent iterations will provide input to the ISMS PDCA cycle by comparison.
- The assessment method should be flexible enough to incorporate new IA aspects as they are identified and modular enough that aspects that no longer need to be monitored can be removed without affecting the validity of other results.
- The methodology should be such that it can be easily, swiftly and periodically administered without overburdening the respondents.
- Different groups of respondents should be catered for.
- Respondents should be authenticated (for reasons that are discussed later in the text) but at the same time,
- Respondent anonymity must be protected.

3. Comparison of Qualitative and Quantitative approaches

For the purposes of the current work, in this section some thoughts are presented on qualitative vs. quantitative research methodologies. The question of the comparative merits of the two approaches constantly surfaces in the social sciences literature, as in Bowling (1997), Babbie (2013) and elsewhere. When an attempt is made to analyse and predict human behaviour, the traditional qualitative approach methods involve observation (Jansen, 2010), participation (Mack et al., 2005), interviews, open-ended questionnaires, closed questionnaires, and, finally, meticulous data analysis.

The detailed comparison of qualitative and quantitative methods is beyond the scope of this paper and it is a subject that has been thoroughly examined by the social scientists. Suffice it to say that a very rich bibliography already exists on the subject and it is constantly expanding. For our purposes, the main comparison aspects are tabulated in the work by Mack et al. (2005) and are being reproduced in Table 1.

	Quantitative	***Qualitative***
General framework	*Seek to confirm hypotheses about phenomena*	*Seek to explore phenomena*
	Instruments use more rigid style of eliciting and categorizing responses to questions	*Instruments use more flexible, iterative style of eliciting and categorizing responses to questions*
	Use highly structured methods such as questionnaires, surveys, and structured observation	*Use semi-structured methods such as in-depth interviews, focus groups, and participant observation*
Analytical objectives	*To quantify variation*	*To describe variation*
	To predict causal relationships	*To describe and explain relationships*
	To describe characteristics of a population	*To describe individual experiences and group norms*
Question format	*Closed-ended*	*Open-ended*
Data format	*Numerical (obtained by assigning numerical values to responses)*	*Textual (obtained from audiotapes, videotapes and field notes)*
Flexibility in study design	*Study design is stable from beginning to end*	*Some aspects of the study are flexible (for example, the addition, exclusion, or wording of particular interview questions)*
	Participant responses do not influence or determine how and which questions researchers ask next	*Participant responses affect how and which questions researchers ask next*
	Study design is subject to statistical assumptions and conditions	*Study design is iterative, that is, data collection and research questions are adjusted according to what is learned*

Table 1: Comparison of quantitative and qualitative research approaches (Mack et al., 2005)

From the comparison presented in table 1, it becomes evident that for the purposes of the proposed methodology as described in section 2 above, quantitative methods appear to meet the set requirements more appropriately.

Qualitative methods cannot effectively be used in the context of the proposed methodology for the following main reasons: 1) The resulting data will be textual and very difficult, if not impossible, to transform into numeric values that indicate the current state-of-play for the information system/structure in question. 2) Due to the open-ended nature of the replies, the resulting data will not be comparable between iterations, thus reducing the value of the exercise for the PDCA cycle. 3) If the qualitative assessment methodology is interview-based, a large number of interviewers who must be specialised/expert both in the field of IA and in interview techniques, will have to be engaged every time the assessment procedure is run, resulting in a serious logistics burden for the Human Resources department and a high overall monetary cost. 4) If the qualitative assessment methodology is questionnaire-based and open-ended, due to the fact that the respondents will have to write extensive answers, the additional burden will make the whole exercise

unattractive to the respondents and this will either lead to inaccurate results from unanswered or hastily answered questions, or the whole process will be met with scepticism and, consequently, will not obtain the acceptance level and necessary support to provide usable results in the long run.

A quantitative, written questionnaire-based approach where a) the questions are pre-determined and are not adapted along the way, as they would be by an interviewer according to the progress of a qualitative interview process, b) the replies are pre-set (i.e. close-ended) and c) discrete numeric values are assigned to them according to a Likert scale (Bowling, 1997) -this is examined in detail later on-, will produce directly comparable results between respondents and between iterations. The variations in the numeric outcomes of the assessment that are caused by IA measures adopted between iterations can thus be quantified. In this manner, the results of the IA effort can be directly assessed, thus allowing for accurate tuning of the overarching ISMS processes. Furthermore, the questionnaires can be easily administered via the organisation's intranet computer network, using existing software tools. Most importantly, the data analysis can be automated to a large extent, immediately yielding directly usable results that can be fed back to the appropriate ISMS modules. Last but not least, all of the above can be done without the extensive engagement of experts that a qualitative approach would require.

Even though the quantitative approach is more appropriate for the work at hand, the value of qualitative research is nevertheless very important in identifying IA weaknesses caused by human behaviour and in providing the necessary groundwork for establishing the quantitative methodology. As already stated, the human aspects of IA identified in previous work by the authors, comprise Social aspects (Frangopoulos et al., 2008), Psychological aspects (Frangopoulos et al., 2010), Psychosocial risk at the workplace (Frangopoulos et al., 2012), Influence techniques and Social Engineering Methods (Frangopoulos, 2007) and choices based on Economic Considerations (Frangopoulos et al., 2014). Luckily, extensive qualitative research has been carried out in the context of the social sciences through well-established self-report methods, as far as the general psychological and social issues are concerned (Kelly, 1955; Llewelyn, 1988; Winter, 1992; Kvale, 1996; Taylor & Bogdan, 1998; Patton, 2002). Insofar the specific context of the human aspects of IA in information systems is concerned, the qualitative approach has been thoroughly examined by Albrechtsen (2007) and others. Thus, most of the necessary qualitative groundwork has already been done, providing a solid foundation for the proposed quantitative approach and the generation of appropriately formed sets of close-ended questions with pre-set, weighted replies.

4. Respondent Groups, authentication and anonymity

In order to carry out an assessment which will yield the best possible results, it will be important to get as many people from the organisation as possible involved in the proposed questionnaire process. Ideally, for 100% precision, the confidence level index "α" should be made equal to 1 (Jansen, 2010), i.e. the total population involved with IA, in any manner, should be included in the process. Apart from that, different

groups of people must be questioned in order to include all of the stakeholders in the assessment process. Questionnaires for each of the groups must be different and the main groups that should be questioned are a) the end-users, b) the Information System administrators, c) the Information Assurance Office personnel, d) the Human Resources Department, and e) representatives of the Management. Although these are the most obvious groups that must be involved, the methodology can be extended to involve any other groups particular to an organisational structure, which might contribute to the assessment process at hand. Such groups could include the infirmary employees (in order to assess psychosomatic issues related to stress and thus the level of the collective psychosocial risk as described by Haubold B., 2008), location security personnel and even cleaning crews. The idea behind the diversity of the various groups is that their diverging activities, roles and responsibilities give them radically different points of view on the same subject. Thus by asking different groups cleverly formulated, but dissimilar, questions on the same subject, the objectivity and accuracy of one group's replies on a particular subject can be judged. Based on Berger & Luckmann's (1991) general position about the problems in communication and understanding between groups of the same structure, it was argued in previous work by the authors (Frangopoulos et al., 2008) that different groups within an information system or information-handling structure, perceive matters differently, thus leading to misconceptions about IA and to a lack of common understanding of IA concepts. This very serious argument is corroborated by the results of the research carried out on the subject by Albrechtsen & Hovden (2009).

To illustrate the necessity of questioning multiple groups, one could consider an example whereby analysis of the data provided by the Management group demonstrates the commitment towards IA, the Information Security Office group data confirm the existence of password policies, the IT administrators group results ascertain the existence of technical measures for password policy enforcement, the end-users group data show compliance to all of the above and, finally, bursting the proverbial bubble, the cleaners group may report workstations that are left logged-on to the system and unattended or sticky yellow notes with funny words written on them on monitors and inside half-open drawers.

A common source of problems in data gathered from questionnaires is the bias created by multiple factors which need to be controlled. Such bias can arise as respondents may choose their replies not based on practice and experience but according to their understanding of what would constitute a "proper" answer. This is described in Barker et al. (2002) as a tendency towards acquiescence (agree rather than disagree) and social desirability (answering in a way that is socially acceptable). In Jones & Nisbet (1971) and Fiske & Taylor (1991), two more potential sources of bias are described: The first is known as the “actor-observer effect” and it refers to people saying that their own behaviour is caused by situational factors and that other people's behaviour is caused by dispositional factors. The second is the “self-serving” bias and it corresponds to the tendency to take credit for success and deny responsibility for failure. Even though there are techniques that mitigate the described bias sources, it can easily be deduced that the error introduced by the above biases is especially grave when the respondent feels pressured or even

threatened by questionnaires not being anonymous. The respondent must never feel that a given reply may have even the remotest chance of being used or interpreted in a way that will affect him/her negatively. The principle of respondent anonymity must thus be upheld at all cost and this must be made crystal-clear to the respondents themselves.

This paramount requirement for anonymity creates all sorts of problems with the administration of the questionnaires, especially when multiple respondent groups are involved. In order to both have respondents answer the proper questionnaire set out for their group and be able to fine tune the iterations of the questionnaire process, each respondent must be identified and authenticated. The authentication requirement has to do with being able to track the participation of respondents in the questionnaire process. As it has already been mentioned, the questionnaire process has to be run iteratively and its results fed to the ISMS. At the same time, it must not create peaks in the collective burden of the organisation. To achieve this, the exercise can be spread out in time as well as among people. The question that arises though is how it can be assured that all (or most) of the respondents participate when requested. This issue can only be dealt with by administrative measures. The necessity for continual awareness education is highlighted in all IA best practices and standards texts such as the ISO 27000 series (ISO/IEC, 2014). This creates, among other administrative difficulties, the problem of tracking each employee's educational record with respect to IA and calling him/her to participate in relevant seminars and other IA awareness actions when the time is due. One way of tackling this is by creating an “IA point system" whereby each employee/respondent must reach a yearly quota of points gained by participating in IA-related activities such as -but not limited to- awareness seminars and assessment procedures (including questionnaires). Such a point system is adopted by the Information Systems Audit and Control Association (ISACA) for allowing its members to retain their hard-earned certifications by remaining continually informed on matters related to Information Security (ISACA, 2014). For such a system to be adopted, it is obvious that the employee/respondent will have to be authenticated in order to have the points awarded to the proper person. This in turn antagonises the much needed concept of anonymity. It should by now be obvious that in order to have respondent authentication combined with anonymity, questionnaire administration will have to adopt specialised anonymisation techniques. The proposed procedure may perhaps be able to borrow elements from existing solutions such as the ones used for collecting sensitive data anonymously for longitudinal research (i.e. correlational research involving repeated observations of the same variables over time), as described in the social sciences literature (Carifio & Biron, 1982; Yurek, Vasey & Havens, 2008; Schnell, Bachteler & Reiher, 2010). This could be combined with solutions proposed in the context of voting systems (Ray & Narasimhamurthi, 2001; Gerck, 2003; Liaw, 2004) whereby the voter is authenticated and given the permission to vote once, his/her vote is recorded, the voting action can be verified, but the vote content is completely disjointed from the voter's identity. In a similar manner, the replies to the questionnaire must be disjointed from the respondent, while the respondent participation is recorded and acted upon, be it for the award of IA points, further iterations of the assessment procedure, the comparative analysis of

group data or for any other action in the context of the IA effort. In this framework, the value of the questionnaire itself as an IA *awareness* tool must not be overlooked as the questionnaire can help the respondent (even at a subliminal level) make sense of the various IA aspects and what these involve, every time the respondent is exposed to a questionnaire's content.

Even with the anonymity of the respondent assured, and other measures against bias errors being in place, the respondents may still choose to answer questions in a "proper" rather than a truthful manner. This is where the matter of question composition comes into play were e.g. potentially sensitive questions should never refer to the respondent's person but rather to the group's general behaviour and characteristics. However, further analysis of this issue goes beyond this paper's scope and will follow in future work.

5. Questionnaire design and administration

It should be clear by now that in order to attain its objectives, the proposed process must be built around a set of very carefully designed questionnaires that take into account the nature of the survey and the individualities of the various respondents.

In order to obtain the required numeric results, a questionnaire based on questions with pre-set (or "close-ended") replies to each of which a discrete numeric value is assigned, must be used. This approach is known as a rating-scale type questionnaire and it is considered to be the central quantitative self-report method (Barker et al., 2002). A variety of rating-scales exist, such as "Thurstone", "Guttman", "Likert" and others (Nunnally & Bernstein, 1994). However, the Likert scale is considered to be the most commonly used in questionnaires of this type (Barker et al., 2002). A discussion of the Likert scale can be found in Bowling (1997) according to whom, when a Likert-type scale is used, the respondent is asked to make judgement on an issue and a discrete numerical value is assigned to that judgement.

Nunnally & Bernstein (1994) argue that the reliability of the result increases with an increase in the dynamic range of the scale, i.e. with more scale points. However, Barker et al. (2002) point out that a dynamic range of more than seven points makes it difficult for respondents to adequately discriminate between them, while Lissitz & Green (1975) consider it useless to have a scale with more than five points.

Likert-type questions can provide quantified results on issues that require the level of respondent agreement with a given statement such as:

How much do you agree with the statement that "you have received adequate Information Assurance training during the past 12 months"?

1 ○	*2* ○	*3* ○	*4* ○	*5* ○
I strongly disagree	*I disagree*	*I neither agree or disagree*	*I agree*	*I strongly agree*

Similarly, an even more direct result on frequency or quantity can be obtained, as shown in the example below:

On a scale of 0 to 6 where 0 represents "never" and 6 "regularly", how often do you find notes with passwords written on them in plain view?

0 ○	*1* ○	*2* ○	*3* ○	*4* ○	*5* ○	*6* ○
Never						*Regularly*

Barker et al. (2002) use the term "central tendency" to describe the phenomenon of respondents avoiding the extreme ends of scales. Thus if the scale ends are avoided, there is not enough dynamic range left in the middle area of the scale to have clearly distinct results. Barker et al. proceed by arguing against a scale of three or four points which may return too many responses in the middle. Hence it seems that the optimal number of points in a Likert scale should be between 5 and 7. Whether it should be an odd number (5 or 7) or an even one (6) has to do with whether a mid-point that represents neutral replies such as "I neither agree nor disagree" is required. The argument for having a mid-point is that respondents should be allowed to express their neutrality. The argument against having a mid-point is that people usually hold an opinion that is not neutral, but may need a little "push" in order to express it. This "push" is accomplished by not giving the respondent a centre point to settle upon (Barker et al., 2002).

It should be borne in mind that it is useful to adopt and use a single type of Likert-scale question throughout the questionnaire as otherwise the respondents may get confused. Thus, if the issues described above are resolved and the question format is decided upon, there are several other matters that must be considered in the design of a questionnaire, as brought to light by Babbie (2013):

a) Sufficient attention must be given to the general format of the questionnaire, in order to not confuse respondents, not cause them to miss questions or even not make respondents reject the whole exercise and throw the questionnaire away. Most importantly, clear instructions must be given to the respondents on what exactly is expected of them and how to reply to the questionnaire.
b) The wording of each question must be such that it does not predispose the respondent towards a particular answer. Additionally, the wording must be such that the question is clear, unambiguous and does not confuse the respondent in any way.
c) Questions should not have multiple parts. Such questions are known as "double-barrelled" and by having more than one parts, they do not allow the respondent to give a focused answer as the respondent may agree with one part of the question and disagree with another. Some conditional questions may also fall in this category and should thus also be avoided. As a practical rule, the word "and" in a question may be making it double-barrelled. That question should thus be broken in two or more distinct questions.
d) Questions should not be arranged in a way that previous questions affect the respondents' replies to subsequent ones.

All of the above must be carefully catered for in the creation of the questionnaires that will be used in the proposed methodology, irrespective of the respondent group that they are distributed to or of the phase during which they are administered. Careful questionnaire design is quintessential to the success of the methodology.

6. Principles and objectives of data gathering and analysis

This section's objective is to set the ground for the possible directions of the analysis of the data that the proposed methodology can provide. The present discussion should neither be seen as an exhaustive approach nor function in a restrictive manner.

It should be borne in mind that each group must be questioned, to the greatest possible extent, on the identified human aspects of IA. It is thus expected that there will be various sets of questions that pertain to each of the identified human aspects areas and to each of the respondent groups. Assuming a) that the questionnaires will be administered over the organisation's intranet and b) that they must not be very time consuming for the respondents, it would be reasonable to administer the questionnaires with only a limited number of different questions each time. Assuming that the questionnaire process has been executed enough times to have obtained a complete first iteration for all subjects from all designated groups, then: a) by comparing the numerical results from different groups on the same subjects, the relative divide on IA issues between groups can be assessed, b) by carefully selecting the questions, their order and the questionnaire phase/section in which they are presented to the respondents, the convergence of what is theoretically understood by the respondents and what their actions prove to have been internalised by them, can be assessed. (In order to do this properly, it is important to be able to attribute replies provided by respondents at different times/phases, to the same, albeit anonymous, individual), c) even from the first time the questionnaire is run in its entirety, several important conclusions about the general IA posture can be drawn, thus identifying the major IA issues that require immediate attention, d) depending on the outcomes of the first iteration, the questionnaire and its deployment can be modified to address newly identified problematic areas during the next iteration. (This must be done in such a controlled way that it does not affect the ability to obtain comparative results on existing, known issues between iterations).

Assuming that the questionnaire procedure has been run at least twice, comparisons between the results obtained from different iterations can be made. Thus, a) conclusions can be drawn on IA-related trends, b) the effects of corrective or preventive IA actions that took place between iterations can be assessed and c) problems of a more general nature may be identified before they become full-fledged IA issues (such as increases in work-related stress, developing conflicting interests among user groups, effects of organisational re-structure etc.).

These outcomes should be used to fuel the virtuous PDCA cycle of the ISMS and provide for changes that may be as important as organisational strategy or policy adjustments. Furthermore, the proposed questionnaire process allows for rapid

internal adjustments, in order to shift its focus towards any issue that attracts the attention of the IA team, most importantly emerging ones. Finally, it should be noted that the expected outcomes described above, should not be seen as an exhaustive list.

7. Conclusions and way forward

In this work, a proposed questionnaire-based methodology is described. This shall form the core of a tool that can provide continuous assessment of the human aspects that affect the IA posture in an organisational structure. Thus, if the "Check" part of the PDCA cycle is visualised as a dashboard on which key parameters and indices, critical for the system at hand, are monitored, the proposed methodology will effectively add another gauge labelled "Human Aspects of IA" to the board. This quantitative methodology is based on sets of different, close-ended, Likert-scale questionnaires that are distributed to various employee groups within an organisation. The comparative analysis of the questionnaire results will provide continuous input to the PDCA virtuous cycle embedded in an ISMS and can help identify emerging human aspect trends before they become full-fledged IA issues. Future actions will include a) the construction of the particular sets of questions which must effectively address problems of respondent-induced bias and inherent questionnaire design difficulties, b) the choice and adaptation of questionnaire administration tools for use over the organisation's intranet and c) the resolution of the matter of respondent identification/authentication combined with anonymity.

8. References

Albrechtsen, E., 2007. A qualitative study of users' view on information security. *Computers & security.* 26(4) pp.276–289.

Albrechtsen, E. & Hovden, J., 2009. The information security digital divide between information security managers and users. *Computers & Security.* 28(6) pp.476–490.

Babbie, E., 2013. *The Practice of Social Research.* 13th ed. Belmont, CA: Wadsworth.

Barker, C., Pistrang, N. & Elliott, R., 2002. *Research Methods in Clinical Psychology: An Introduction for Students and Practitioners*. 2nd ed. Chichester, UK: John Wiley & Sons, Ltd.

Berger, P.L. & Luckman, T., 1991. *The social construction of reality. A treatise in the sociology of knowledge*. London: Penguin Books.

Bowling A., 1997. Questionnaire design. In: *Research Methods in Health.* Buckingham: Open University Press.

Carifio, J. & Biron, R., 1982. Collecting sensitive data anonymously: Further findings on the CDRGP technique. *Journal of Alcohol and Drug Education.* 27(2) pp.38-70.

Deming, W.E., 1986. *Out of the crisis*. Cambridge, MA: Massachusetts Institute of Technology , Center for Advanced Engineering Study.

Fiske, S.T. & Taylor, S.E., 1991. *Social cognition.* 2nd ed. New York: McGraw-Hill.

Frangopoulos, E.D., 2007. *Social Engineering and the ISO/IEC 17799:2005 Security Standard: A Study on Effectiveness*,. MSc Dissertation, University of South Africa.

Frangopoulos, E.D., Eloff, M.M. and Venter, L.M., 2008. Social aspects of Information Security. In: *Proceedings of the Information Security South Affrica (ISSA) 2008 Innovative Minds Conference*. Gauteng Region (Johannesburg), South Africa, 2-4 July 2008.

Frangopoulos, E.D., Eloff, M.M. and Venter, L.M., 2010. Psychological Considerations in Social Engineering – The Ψ-Wall as defence. *IADIS International Journal on Computer Science and Information Systems.* 5(2) pp.1-20.

Frangopoulos, E.D., Eloff, M.M. and Venter, L.M., 2012. Psychosocial Risks: can their effects on the Security of Information Systems really be ignored? In: Clarke N.L. and Furnell S.M. (ed.) 2012. *Proceedings of the Sixth International Symposium on Human Aspects of Information Security and Assurance (HAISA) 2012.* Crete, Greece, 6-8 June 2012.

Frangopoulos, E.D., Eloff, M.M. and Venter, L.M., 2014 (in press). Information Security Economics: Induced Risks and Latent Costs. In: *Proceedings of the 13th European Conference on Cyber Warfare and Security ECCWS-2014.* Piraeus, Greece, 2-4 July 2014. (Accepted for publication February 2014).

Gerck, E., 2003. Private, secure and auditable Internet voting. In *Secure Electronic Voting,* pp. 165-179. Springer US.

Haubold B., 2008. *Les risques psychosociaux. Identifier, analyser, prévenir les risques humains*. Paris: Éditions d' Organisation Groupe Eyrolles.

ISACA, 2014. *CISM Continuing Professional Education (CPE) Policy* [pdf]. ISACA. [online] Available at: <http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Maintain-Your-CISM/Documents/CISM-CPE-English.pdf> [Accessed 1 April 2014].

ISO/IEC, 2014. *International Standard ISO/IEC 27000:2014. Information technology - Security techniques - Information security management systems - Overview and vocabulary.* Geneva: ISO Copyright Office.

Jansen, H., 2010. The Logic of Qualitative Survey Research and its Position in the Field of Social Research Methods. In: *Forum: Qualitative Social Research,* 11(2).

Jones, E.E. & Nisbett, R.E., 1971. The actor and the observer: Divergent perceptions of the causes of behaviour. In Jones, E.E., Kanouse, D.E., Kelley, H.H., Nisbett, R.E., Valins, S. & Weiner, B. (eds). *Attribution: Perceiving the causes of behaviour*. Morristown, NJ: General Learning Press.

Kelly, G.A., 1955. *The psychology of personal constructs*. New York: Norton.

Kvale, S., 1996. *Interviews: An introduction to qualitative research interviewing.* Thousand Oaks, CA: Sage.

Liaw, H. T., 2004. A secure electronic voting protocol for general elections. *Computers & Security*, 23(2), pp.107-119.

Lissitz, R.W. & Green, S.B., 1975. Effect of the number of scale points on reliability: A Monte Carlo approach. *Journal of Applied Psychology*, 60, pp.10–13.

Llewelyn, S.P., 1988. Psychological therapy as viewed by clients and therapists. *British Journal of Clinical Psychology*, 27, pp.223–237.

Mack, N., Woodsong, C., MacQueen, K. M., Guest, G. & Namey, E., 2005. *Qualitative research methods: a data collectors field guide.* Research Triangle Park, North Carolina, USA: Family Health International [FHI].

Nunnally, J. C., & Bernstein, I. H., 1994. *Psychometric theory.* 3rd ed. New York, NY: McGraw-Hill.

Patton, M.Q., 2002. *Qualitative research and evaluation methods.* 3rd ed. Thousand Oaks, CA: Sage.

Ray, I., & Narasimhamurthi, N., 2001. An anonymous electronic voting protocol for voting over the internet. In *Advanced Issues of E-Commerce and Web-Based Information Systems, WECWIS 2001, Third International Workshop on,* pp.188-190.

Schneier, B., 2000. *Secrets & Lies*. USA: John Wiley & Sons Inc.

Schnell, R., Bachteler, T., & Reiher, J., 2010. Improving the use of self-generated identification codes. *Evaluation review*, 34(5), pp.391-418.

Taylor, S.J. & Bogdan, R., 1998. *Introduction to qualitative research methods: A guidebook and resource*. 3rd ed. New York: Wiley.

Winter, D.A., 1992. *Personal construct psychology in clinical practice*. London: Rutledge.

Yurek, L.A., Vasey, J., & Havens, D.S., 2008. The use of self-generated identification codes in longitudinal research. *Evaluation review*, 32(5), pp.435-452.