Bibliography

Albrechtsen, E. 2007. A qualitative study of users' views on information security. *Computers and Security*, 2007(26): 276-289.

Andress, M. 2000. Manage people to protect data. *InfoWorld*, 22(46): 48.

Andric, M. 2007. Fighting the enemy within. *IT WEB Special Report*, April 2007(95): 54.

Ashkanasy, N.M., Wilderom, C.P.M. & Peterson, M.F. (eds). 2000. *Handbook of organisational culture & climate.* California: Sage Publications.

Baggett, W.O. 2003. Creating a culture of security. *The Internal Auditor*, (60)3: 37-41.

Berry, M.L. & Houston, J.P. 1993. *Psychology at work.* Wisconsin: Brown and Benchmark Publishers.

Borking, J. 2006. Without privacy standards no trust in and outside cyberspace. Retrieved online on 25 April 2008 from https://www.prime-project.eu/events/standardisation-ws/slides/Withoutprivacynotrust-JohnBorking.pdf/file_view

Bresz, P.F. 2004. People – often the weakest link in security, but one of the best places to start. *Journal of Health Care Compliance*, (6)4: 57-60.

Brewerton, P. & Millward, L. 2002. *Organizational research methods*. London: Sage Publications.

BS 7799 (BS 7799-2). 2002. *Information technology*. Security techniques. Information security management systems – requirements.

Chau, P.Y.K. 1999. On the use of construct reliability in MIS research: a meta-analysis. *Information Management*, (35)4: 217-227.

Cardinali, R. 1995. Reinforcing our moral vision: Examining the relationship between unethical behaviour and computer crime. *Work Study*, 44(8): 11-18.

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

CISA Review Manual. 2005. ISACA: Rolling Meadows.

COBIT security baseline – An information security survival kit. 2004. USA: IT Governance Institute.

Connolly, P.J. 2000. Security starts from within. *InfoWorld,* 22(28): 39-40.

Da Veiga, A., Martins, N. & Eloff, J.H.P. 2007. Information security culture – validation of an assessment instrument. *Southern Africa Business Review*, (11)1: 146-166.

Deloitte & Touche LLP, Ernst & Young LLP, KPMG LLP & PricewaterhouseCoopers LLP. 2004. Perspectives on Internal Control Reporting - a Resource for Financial Market Participants. Retrieved online on 18 January 2007 from http://www.ey.com/global/download.nsf/

Dervin, L., Kruger, H. & Steyn, T. 2006. Value-focused assessment of information communication and technology security awareness in an academic environment. **In** IFIP International Federation for Information Processing, *Security and Privacy in Dynamic Environments*, 201: 448-453.

Detert, J.R., Schroeder, R.G. & Mariel, J. 2000. A framework linking culture and improvement initiatives in organisations. *The Academy of Management Review*, 25(4): 850-863.

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

Dojkovski, S., Lichtenstein, S. & Warren, S. 2006. Fostering information security culture in small and medium size enterprises: An interpretive study in Australia. Retrieved online on 8 August 2007 from http://csrc.lse.ac.uk/asp/aspecis/20070041.pdf

Donaldson, W.H. 2005. U.S. Capital Markets in the Post-Sarbanes-Oxley World: Why Our Markets Should Matter to Foreign Issuers. Chairman, U.S. Securities and Exchange Commission. London School of Economics and Political Science.

Electronic Communications and Transactions Act (ECTA). 2002. Retrieved online on 12 January 2006 from http://www.acts.co.za/ect_act/

Eloff, J.H.P. & Eloff, M. 2005. Integrated Information Security Architecture, *Computer Fraud and Security*, 2005(11): 10-16.

Finance. 2008. Retrieved online on 22 August 2008 from www.finance.gov.au/gateway/guidance_glossary.html.

Flowerday, S. & Von Solms, R. 2006. *Trust an element of information security*. In *Security and Privacy in Dynamic Environments*. IFIP/SEC2005. Boston: Kluwer Academic Publishers, 87-97.

Furnell, S.M. 2004. Enemies within: the problem of insider attacks. *Computer Fraud & Security*. 2004(July): 6-11.

Furnell, S.M. 2007. IFIP workshop – Information security culture. *Computers and Security*, 2007(26): 35.

Furnham, A. & Gunter, B. 1993. *Corporate assessment: Auditing a company's personality*. London: Routledge.

Gaunt, N. 2000. Practical approaches to creating a security culture. *International Journal of Medical Informatics*, 60(2): 151-157.

Grant, R. 2005. Building a strong security culture. Retrieved online on 16 January 2006 from http://www.citec.com.au/news/featureNews/2005/April/security_culture.shtml?rate

Guldenmund, F.W. 2000. The nature of safety culture: A review of theory and research. *Safety Science*, 34: 215-257.

Hall, E.M. 1998. *Managing risk: Methods for software systems development.* Reading: Addison-Wesley.

Health Insurance Portability & Accountability Act. (HIPAA). 2006. Retrieved online on 1 August 2006 from http://www.asksam.com/ebooks/hipaa/

Helle, A.J. 2005. Security culture and risk management is a management responsibility. Retrieved online on 16 January 2006 from http://64.233.161.104/search?q=cache:iz7ehU05geYJ:www.telenor.com/telektronikk/volumes/pdf/1.2005/Page_011-014.pdf+information%2Bsecurity%2Bculture&hl=en

Hellriegel, D., Slocum, Jr. J.W. & Woodman, R.W. 1998. *Organizational behavior*. Eighth edition. South-Western College Publishing.

Helokunnas, T. & Kuusisto, R. 2003. Information Security Culture in a Value Net. In *2003 IEEE International Engineering Management Conference*, Albany, New York.

Helokunnas, T. & Ilvonen, I. 2004. Information security culture in small and medium sized enterprises. Retrieved online on 16 January 2006 from http://64.233.161.104/search?q=cache:BQkgIbn4EawJ:www.ebrc.info/kuvat/2034.pdf+information%2Bsecurity%2Bculture&hl=en

Hintze, J.L. 1997. Number Cruncher Statistical Systems, version 5.03 5/90. Kaysville, UT: NCSS.

Howell, D.C. 1995. Fundamental statistics for the behavioral sciences. 3rd International Standards Organisation. Retrieved online in January 2005 from http://www.iso.ch

Huysamen, G.K. 1988. *Sielkundige meting – 'n Inleiding*. Pretoria: J.L. van Schaik.

Information Security Forum. 2000. *Information Security Culture – A preliminary investigation.* s.l

Information Security Forum. 2003. *Standard of Good Practice for Information Security.* s.l.

Information Security Forum. 2008. Retrieved online on 11 February 2008 from www.securityforum.org

ISACA. 2008. Information Systems Audit and Control Association. http//:www.isaca.org

ISO/IEC 17799 (BS 7799-1). 2000. *Information technology. Security techniques. Code of practice for information security management.*

ISO/IEC 17799 (BS 7799-1). 2005. *Information technology. Security techniques. Code of practice for information security management*.

ISO/IEC 27001 (BS 7799-2). 2005. *Information technology. Security techniques. Information security management systems – requirements*.

King Report II. 2001. The King Report of corporate governance for South Africa. Retrieved online on 12 January 2006 from http://www.iodsa.co.za/downloads/King%20II%20Report%20CDRom%20Brochure.pdf

Kraemer, S. & Carayon, P. 2005. Computer and Information security culture – findings from two studies. **In** *Proceedings of the human factors and ergonomics society 49th annual meeting.* Retrieved online on 20 July 2007 from http://ecow.engr.wisc.edu/cgi-bin/get/ie/705/karsh/readings/hfesorland/kraemeruw-madison2005.pdf

Kraemer, S. & Carayon, P. 2007. Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics*, 38(2007): 143-154.

Kraemer, S., Carayon, P. & Clem, J.F. 2006. Characterising violations in computer and information security systems. Retrieved online on 20 June 2007 from http://cqpi2.engr,wisc.edu/cis/docs/skiea2006.pdf.

Kraut, A.I. 1996. *Organizational Surveys*. San Francisco: Jossey-Bass Publishers.

Kreitner, R. & Kinicki, A. 1995*. Organizational behavior*. Chicago: IRWIN Inc.

Krejcie, R.V. & Daryle, M.W. 1970. Determining sample size for research activities. *Educational and Psychological Measurement, 1970(30): 607-610.*

Kruger, H.A. & Kearney, W.D. 2006. A prototype for assessing information security awareness. *Computers & Security*, 25(2006): 289-296.

Kuusisto, R. & Ilvonen, I. 2003. Information security culture in small and medium-sized enterprises. *Frontiers of E-business Research.* Retrieved online on 20 June 2007 from http://www.ebrc.fi/kuvat/431-439.pdf

Le Grand, C. & Ozier, W. 2000. Information Security Management Elements. Retrieved online on 20 March 2000
from http://www.itaudit.org/forum/auditcontrol/f305ac.htm

Lundy, O. & Cowling, A. 1996. *Strategic human resource management*. London: Routledge.

Magklaras, G.B. & Furnell, S.M. 2004. A preliminary model of end user sophistication for insider threat prediction in IT systems. *Computers & Security*, 25(2006):27-35.

Martins, A. 2002. *Information security culture*. Johannesburg: Rand Afrikaans University. (M.Com thesis.)

Martins, A. & Eloff, J.H.P. 2002. Information security culture. In *Security in the information society*. IFIP/SEC2002. Boston: Kluwer Academic Publishers: 203-214.

Martins, N. & von der Ohe, H. 2003. Organisational climate measurement – new and emerging dimensions during a period of transformation. *South African Journal of Labour Relations*, (27)3 and 4: 41-59.

McCarthy, M.P. & Campbell, S. 2001. *Security transformation*. New York: McGraw-Hill.

McHaney, R., Hightower, R. & Pearson, J. 2002. A validation of end-user computing satisfaction instrument in Taiwan. *Information Management*, (39)6: 503-511.

McIlwrath, A. 2006. *Information security and employee behaviour*. Hampshire: Gower.

NCSU. 2008. Retrieved online on 22 August 2008 from www.ncsu.edu/scrc/public/DEFINITIONS/G%20-%20I.html

Nosworthy, J.D. 2000. Implementing information security in the 21st century – do you have the balancing factors? *Computers and Security*, 19(4): 337-347.

Odendaal, A. 1997. *Deelnemende bestuur en korporatiewe kultuur: onafhanklike konstrukte? / Participative management and corporate culture: independent constructs?* Rand Afrikaans University: Johannesburg. (MA thesis.)

Olivier, M.S. 1999. *Information Technology Research – A practical guide.* Rand Afrikaans University: Johannesburg.

Pfleeger, C.P. 1997. *Security in computing*. Second edition. New Jersey: Prentice Hall.

Pocket Oxford Dictionary 1.0. 2005. Retrieved online on 1 January 2008 from http://freedownloadscentre.com/Palm_Pilot/Utilities/Pocket_Oxford_English_Dictionary.html

Posthumus, S. & Von Solms, R. 2005. IT Governance. *Computer Fraud and Security*, 2005(6): 11-17.

Puhakainen, P. 2006. A design theory for information security awareness. Retrieved online 31 July 2008 from http://herkules.oulu.fi/isbn9514281144/isbn9514281144.pdf.

PriceWaterhouseCoopers. Information security breaches survey. 2004. Retrieved online on 12 March 2005 from http://www.dti.gov.uk/industry_files/pdf/isbs_2004v3.pdf

Promotion of Access to Information Act (PROATIA). 2000. Retrieved online on 12 January 2006 from http://www.acts.co.za/prom_of_access_to_info/index.htm

Purser, S. 2004. Integrating security into the corporate culture. Retrieved online on 16 January 2006 from http://www.infosecwriters.com/texts.php?op=display&id=249

Rees, J., Bandyopadhyay, S. & Spafford, E. 2003. PFIRES: A policy framework for information security. *Communications of the ACM*, (46)7: 101-106.

Robbins, S.P. 1997. *Organizational behaviour*, 5th ed. New Jersey: Prentice Hall.

Robbins, S.P. 1998. *Organizational behaviour.* 8th ed. New Jersey: Prentice Hall.

Robbins, S. 2001. *Organizational behaviour*. 9th ed. New Jersey: Prentice Hall.

Robbins, S., Odendaal, A. & Roodt, G. 2003. *Organisational behaviour – Global and Southern African perspectives.* Pearson Education South Africa: Cape Town.

Ruighaver, A.B. & Maynard, S.B. 2006. Organisational security culture: More than just an end user phenomenon. **In** *IFIP International Federation for Information Processing*, Security and Privacy in Dynamic Environments, 201: 425-430.

Ruighaver, A.B., Maynard S.B. & Chang, S. 2006. Organisational security culture: Extending the end-user perspective. *Computers and Security,* 2007(26): 56-62.

Sartor, R. 2008. Privacy, reputation and trust: Some implications for data protection. Retrieved online on 25 April 2008 from http://www2.cirsfid.unibo.it/~sartor/GSCirsfidOnlineMaterials/GSOnLinePublications/GSPUB2006PrivacyReputationTrust.pdf

SAS. 2008. Statistical Analysis Software. Retrieved online on 31 July 2008 from http://www.sas.com/technologies/analytics/statistics/stat/index.html.

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

Schermelleh-Engel, K., Moosbrugger, H. & Muller, H. 2003. Evaluating the fit of structural equation models: Test of significance and descriptive goodness-of-fit measures. *Methods of Psychological Research Online*. 8(2): 23-74.

Schiesser, R. 2002. *IT systems management*. Upper Saddle River: Prentice Hall.

Schlienger, T. 2006. *Informationssicherheitskultur in Theorie und Praxis: Analyse und Förderung sozio-kultureller Faktoren der Informationssicherheit in Organisationen.* iimt University Press: Fribourg. (Published D. Phil. thesis)

Schlienger, T. & Teufel, S. 2002. Information security culture. **In** *Security in the Information Society.* IFIP/SEC2002. Boston: Kluwer Academic Publishers: 191-201.

Schlienger, T. & Teufel, S. 2003a. Information security culture: from analysis to change. **In** *Information Security South Africa – Proceedings of ISSA 2003, 3rd Annual Information Security South Africa Conference*. South Africa. ISSA: 183-195

Schlienger, T. & Teufel, S. 2003b. Analysing information security culture: Increased trust by an appropriate information security culture. **In** *International Workshop on Trust and Privacy in Digital Business Trust Bus'03) in conjunction with 14th International Conference on Database and Expert Systems Applications (14th: 2003: Prague)*. Czech Republic.

Schlienger, T. & Teufel, S. 2005. Tool supported management of information security culture. **In** *IFIP International Information Security Conference (20th: 2005: Makuhari-Messe, Chiba)*. Japan.

Sherwood, J., Clark, A. & Lynas, D. 2005. *Enterprise security architecture. A business-driven approach.* CMP Books: Berkeley.

Siponen, M., Pahnila, S. & Mahmood, A. 2007. Employees' adherence to information security policies: An empirical study. **In** *Proceedings of New*

Approaches to Security, Privacy and Trust in Complex Environments, FIP/SEC2007, Sandton, South Africa: 133-144.

SSE-CMM. 2008. Systems Security Engineering Capability Maturity Model. Retrieved online on 31 July 2008 from http://www.sse-cmm.org/index.html

Standard of Good Practice. 2003. Information Security. Information Security Forum. Retrieved online on 20 February 2008 from https://www.securityforum.org/html/frameset.html

Stanton, J.M., Stam, K.R., Mastrangelo, P. & Jolton, J. 2005. Analysis of end user security behaviours. *Computers and Security*, (24)2: 124-133.

Starnes, R. 2006. Creating a security culture. Retrieved online on 16 January 2006 from http://www.cw.com/uk/solutions/business/risk_security/story_0501004_starnes.html

Stewart, J.N. 2006. CSO to CSO: Establishing the security culture begins at the top. Retrieved online on 16 January 2006 from http://cisco.com/web/about/security/intelligence/05_07_security-culture.html

Straub, D. 1989. Validating instruments in MIS research. *MIS Quarterly*, (13)2: 147-169.

Straub, D.W. 1990, Effective IS security: an empirical study. *Information Systems Research*, (1)3: 255-276.

Straub, D., Boudreau, M. & Gefen, D. 2004. Validation guidelines for IS positivist research, *Communications of the Association for Information Systems*, (13)24: 380-427.

Survey Tracker. 2008. Retrieved online on 23 January 2008 from http://www.surveytracker.com

Tessem, M.H. & Skaraas, K.R. 2005. Creating a security culture. Retrieved online on 16 January 2006 from http://www.telenor.com/telektronikk/volumes/pdf/1.2005/Page_015-022.pdf

The Concise Oxford Dictionary. 1983. Oxford: Clarendon Press.

The promotion of a culture of security for information systems and networks in OECD countries (OECD), DSTI/ICCP/REG(2005)1/FINAL.2005. Retrieved online on 8 August 2006 from http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html

Thomson, I. 2004. IT security culture must start from the top – Global survey warns senior execs against 'delegating' security awareness. Retrieved online

on 16 January 2006 from
http://www.vnunet.com/vnunet/news/2125904/security-culture-start-top

Thomson, K. & Von Solms, R. 2005. Information security obedience: a definition. *Computers and Security*, 2005(24): 69-75.

Thomson, K., Van Solms, R. & Louw, L. 2006. Cultivating an organisational information security culture. *Computer Fraud and Security,* October (2006): 7-11.

Thomson, K. & Von Solms, R. 2006. Towards an information security competence maturity model. *Computer Fraud and Security*, 2005(5): 11- 14.

Trček, D. 2003. An integral framework for information systems security management. *Computers and Security*, 22(4): 337-360.

Trompeter, C.M. & Eloff, J.H.P. 2001. A framework for the implementation of socio-ethical controls in Information Security. *Computers and Security*, 20(5): 384-391.

Tudor, J.K. 2000. *Information Security Architecture – An integrated approach to security in an organisation*. London: Auerbach.

Tudor, J.K. 2006. *Information security architecture - An integrated approach to security in organisations*. Boca Raton: Auerbach.

Van der Merwe, P. & Cantale, S. 2007. Cyber-baddies make jay as CIOs snooze. *Brainstorm*, 6(9): 59-66.

Van der Raadt, B., Soetendal, J., Perdeck, M. & Van Vliet, K. 2004. Polyphony in architecture. **In** *Proceedings of the 26th International Conference on Software Engineering (ICSE'04).* IEEE.

Van Niekerk, J. & Von Solms, R. 2005. An holistic framework for the fostering of an information security sub-culture in organizations. **In** *Information Security South Africa – Proceedings of ISSA 2005, 4th Annual Information Security South Africa Conference. South Africa.* Retrieved online on 16 March 2008 from http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/041_Article.pdf

Van Niekerk, J. & Von Solms. R. 2006. Understanding information security culture: A conceptual framework. **In** *Information Security South Africa – Proceedings of ISSA 2006, 5th Annual Information Security South Africa Conference. South Africa.* Retrieved online on 16 March 2008 from http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/21_Paper.pdf

Verton, D. 2000. Companies aim to build security awareness. *Computerworld,* 34(48): 24.

Von Solms, B. 2000. Information security – The third wave? *Computers and Security,* 19(7): 615-620.

Von Solms, B. 2005. Information security governance – compliance management versus operational management. *Computers and Security*, (24)6: 443-447.

Von Solms, B. 2006. Information security – The fourth wave. *Computers and Security*, 25(2006): 165-168.

Von Solms, R. & Von Solms, B. 2003. From policies to culture. *Computers and Security,* (2004)23: 275-279.

Von Solms, R. 1998. Information security management (3): The code of practice for information security management (BS7799). *Information Management and Computer Security,* 6(5): 224-225.

Vroom, C. & Von Solms, R. 2004. Towards information security behavioural compliance. *Computers and Security,* (23)3: 191-198.

Walters, M. 1996. *Employee attitude and opinion surveys*. London: Institute of Personnel and Development.

Walton CB, R., & Walton-Mackenzie Limited. 2006. Balancing the insider and outsider threat. *Computer Fraud and Security*, 2006(11): 8-11.

Whitman, M.E. & Mattord, H.K. 2003. *Principles of information security.* Kennesaw State University: Thomson Course Technology.

Willison, R. & Siponen, M. 2007. A critical assessment of IS security research between 1990-2004. **In** *Proceedings of the 15th European Conference of Information Systems,* St. Gallen, Switzerland, June 7-9, 2007.

Witty, R.J. & Hallawell, A. 2003. Client issues for security policies and architecture. Gartner. ID number: K-20-7780.

Woon, I.M.Y., Tan, G.W. & Low, R.T. 2005. A protection motivation theory approach to home wireless security. **In** *Proceedings of the twenty-sixth International Conference on Information Systems*, Las Vegas, 367-380.

Workman, M., Bommer, W.H. & Straub, D. 2008. Security lapses and the omission of information security measures: A threat control model and empirical test, *Computers in Human Behaviour*, Article in press – corrected proof. Retrieved online on 31 July 2008 from http://www.sciencedirect.com.

Yang, Z., Cai, S., Zhou, Z. & Zhou, N. 2005. Development and validation of an instrument to measure user perceived service quality of information presenting web portals. *Information & Management*, (42)4: 575-589.

Zachman, J. 2008. *Zachman framework*. Retrieved online on 8 February 2008 from http://www.zifa.com/

Zakaria, O. 2006. Internalisation of information security culture amongst employees through basis security knowledge. **In** *IFIP International Federation for Information Processing,* Security and Privacy in Dynamic Environments. Fisher-Hübner, S., Rannenberg, K., Yngström L. & Lindskog, S. (eds). 201: 437-441.

Zakaria, O. & Gani, A. 2003. A conceptual checklist of information security culture. **In** *Proceedings of the 2nd European Conference on Information Warfare and Security*, Reading, UK.

APPENDICES

APPENDIX A – INFORMATION SECURITY CULTURE ASSESSMENT INSTRUMENT

APPENDIX B – INITIAL INFORMATION SECURITY CULTURE ASSESSMENT INSTRUMENT (DA VEIGA, MARTINS & ELOFF, 2007)

APPENDIX C – INFORMATION SECURITY CULTURE ASSESSMENT REPORT

APPENDIX D – PAPER PUBLISHED IN JOURNAL: INFORMATION SECURITY CULTURE – VALIDATION OF AN ASSESSMENT INSTRUMENT

Information security culture – validation of an assessment instrument

A. da Veiga, N. Martins & J.H.P. Eloff

ABSTRACT

Organisations need to ensure that the interaction among people, as well as between people and information technology (IT) systems, contributes to the protection of information assets. Organisations therefore need to assess their employees' behaviour and attitudes towards the protection of information assets in order to establish whether employee behaviour is an asset or a threat to the protection of information. One approach that organisations could use is to assess whether an acceptable level of information security culture has been inculcated in the organisation and, if not, take corrective action. The aim of this paper is to validate an information security culture assessment instrument. This is achieved by performing a factor and reliability analysis on the data from an information security culture assessment in a financial organisation. The results of the analysis are used to identify areas for improving the information security culture assessment instrument. The study makes a contribution to the existing body of knowledge concerned with the assessment of information security culture and its value for management to ensure the protection of information assets.

Key words: information security, information security culture, information security awareness, behaviour, measure, assess, questionnaire, validity, reliability, survey

INTRODUCTION

Information security encompasses technology, processes and people (Von Solms 2000; Tessem & Skaraas 2005). It comprises a suitable set of controls such as organisational structures, software principles and e-mail practices implemented by the organisation. These information security controls are implemented to ensure the confidentiality,

Ms A. da Veiga and Prof. J.H.P. Eloff are in the Information and Computer Security Architectures Research Group, Department of Computer Science, University of Pretoria. Prof. N. Martins is in the Department of Industrial Psychology, University of South Africa. E-mail: adele.daveiga@kpmg.co.za

integrity and availability of the organisation's information, which may be essential to maintaining a competitive edge, cash flow, profitability or legal compliance (ISO 2005).

Many organisations are at the stage where they have implemented technology and compiled information security policies and procedures to protect the organisation's information from a wide variety of threats. These threats could vary from computer-assisted fraud, espionage, sabotage and vandalism to fire. According to the Control Objectives for Information and related Technology (COBIT) Security Baseline Survival Kit (COBIT 2004), a lack of security awareness could cause a gap in an organisation's implementation of information security. Organisations now have to ensure that employees are aware of their responsibility in securing information assets such as archived information, system documentation, business strategies and databases (COBIT 2004; ISO 2005). Employees must also be adequately trained in order for the organisation to direct their behaviour to minimise accidental and malicious threats to information assets. The ISO17799 (ISO 2005) standard states that "providing appropriate training, education and awareness" is critical to the successful implementation of information security. It is therefore important that the members of an organisation's workforce are aware and conscious of information security in their daily work activities. In each organisation, an information security culture will emerge over time and become evident in the behaviour and activities of the workforce. This information security culture that develops can be defined as the assumption about those perceptions and attitudes that are accepted and encouraged in order to incorporate information security characteristics as the way in which things are done in an organisation, with the aim of protecting information assets (Martins & Eloff 2002; Martins 2002). For organisations to manage security risks to information assets, they must have a strong information security culture (Baggett 2003; CITEC 2005; Dervin, Kruger & Steyn 2006; Gaunt 2000; ISF 2000; Martins & Eloff 2002; Ruighaver & Maynard 2006; OECD 2005; Stewart 2006; Schlienger & Teufel 2005; Tessem & Skaraas 2005; Thomson 2004; Von Solms 2006; Zakaria 2006).

Various factors motivate the importance of inculcating an information security culture in order to protect the information assets of organisations. The people who are expected to be responsible for information security constitute one of the main factors in this equation. Research illustrates that the interaction of people and the behaviour of employees towards computer and information assets represent the weakest link in information security (Abu-Musa 2003; Baggett 2003; Bresz 2004; Martins & Eloff 2002; Schlienger & Teufel 2002).

Based on a survey conducted by PricewaterhouseCoopers in 2004 (PWC 2004), a comparison was made between various surveys to illustrate the number of organisations that had experienced a security incident. As many as 83% of respondents indicated that they had experienced high-technology information security incidents. The three most common breaches were virus infections, staff

misuse of the Internet and physical theft of computer equipment. Although the number of technology incidents was very high, the report stated that "human error rather than technology is the root cause of most security breaches" (PWC 2004). According to PricewaterhouseCoopers, the solution would be to create a security-aware culture. Staff should be made more aware of the risks and of their responsibilities, thereby enabling them to act in a sensible and secure manner. The Guidelines for Security of Information Systems and Networks (Baggett 2003; OECD 2005) of the Organisation for Economic Cooperation and Development (OECD) provide a comprehensive framework for creating a culture of security. Through principles such as awareness, responsibility and ethics, a security culture will begin to develop – thereby minimising the threat that users pose to computer assets.

The organisation thus needs to ensure that an information security culture is inculcated through training, education and awareness in order to minimise risks to information assets. To determine whether the information security culture is at an acceptable level, it needs to be measured and reported on. One way of measuring the level of an organisation's information security culture is to use an information security culture assessment instrument (questionnaire) (Martins & Eloff 2002; Martins 2002; Schlienger & Teufel 2005). The results obtained from such an assessment can be used to identify areas for improving the protection of information assets.

AIM OF THIS PAPER

The aim of this paper is to validate an assessment instrument for assessing information security culture and provide one that is accepted as a valid and reliable assessment instrument in the information security and psychology research fields. In order to achieve the aim of the paper, an information security culture assessment was conducted in a financial organisation using an information security culture questionnaire.

CURRENT DEVELOPMENTS IN INFORMATION SECURITY CULTURE ASSESSMENTS

Perspective of the Information Security Forum

During November 2000, the Information Security Forum (ISF 2000) released a report discussing the definition of information security culture and the factors on which to focus when measuring it. They started their research in the realisation that despite compelling evidence that well-directed action can reduce information risks, incidents continue to occur on a daily basis. They concluded that this was probably due to a lack of a strong information security culture for driving down risk.

Based on the research work that the ISF conducted, they propose to develop a questionnaire to measure information security culture (ISF 2000). The main objective of the questionnaire would be for an organisation to identify the effect of information security culture on the organisation's level of information risk and specific target areas for improvement. As part of the ISF's future work, they plan to pilot the questionnaire at member firms, standardise it, enable benchmarking between organisations, and develop an implementation guide for organisations to use the measurement tool (ISF 2000).

Perspective of Schlienger and Teufel

Schlienger & Teufel (2002) introduced a paradigm shift – from a technical approach, towards information security, to a socio-cultural approach. They concluded that one has to focus on the organisational culture in addressing the human element so as to minimise risks to information assets and concentrate on the information security culture of the organisation.

Schlienger & Teufel (2003; 2005) selected the survey method, using a questionnaire, to obtain an understanding of the official rules that are supposed to influence the security behaviour of employees. Schlienger & Teufel's (2005) questionnaire takes into account the three levels of organisational behaviour of Robbins (2001), as well as research work performed by Schein (1985). It measures 20 areas (for example, leadership, problem management, communication and attitude). They performed substantive research to develop a decision-support system for analysing the results automatically and enabling employees to complete the questionnaire online. This tool was implemented in a private bank, and the application illustrated its usefulness. The Working Group on Information Security Culture of the Information Security Society of Switzerland (FGSec) also participated through discussions to ensure the practicability of the process. Schlienger & Teufel further aim to focus on extending the tool to allow benchmarking (Schlienger & Teufel 2005).

Perspective of Martins and Eloff

Martins and Eloff (Martins 2002; Martins & Eloff 2002) designed an information security culture model based on the concepts of organisational behaviour (Robbins, Odendaal & Roodt 2003) and what constitutes information security. They identified information security controls at the individual, group and organisational levels of organisational behaviour that could influence information security culture (Martins 2002; Martins & Eloff 2002). This theoretical perspective provided the basis for the information security culture questionnaire and the items developed by the researchers to assess information security culture (Martins 2002; Martins & Eloff 2002). The

information security culture questionnaire, however, still needs to be statistically standardised through a large enough sample so as to provide data that can be used to conduct a factor and reliability analysis that will ensure its validity and reliability.

MEASURING INSTRUMENT

The purpose of this paper is to validate the assessment instrument developed by Martins & Eloff (2002) and Martins (2002). The information security culture questionnaire developed by Martins & Eloff was selected, as it is based on an information security culture model addressing content validity (Brewerton & Millward 2001); moreover, its usefulness and practicality had already been proven in a case study (Martins 2002, Martins & Eloff 2002). This questionnaire was developed for use in environments where awareness programmes had already been implemented, as well as those where such programmes had not previously been implemented. It could therefore be applied in financial organisations, even if they had not implemented any awareness programmes. In addition, the information security culture questionnaire includes knowledge questions that are analysed separately from the information security culture statements. These questions assess awareness of employees pertaining to information security requirements that management expects employees to know. The knowledge questions can be used to obtain information pertaining to current knowledge of employees that could result in specific behaviour. If an employee does not know what an information security incident is, one could argue that he/she will not effectively report such incidents. This contributes to the practicability of the questionnaire, as the financial organisation specifically required the knowledge questions to determine how much employees know about information security in order for management to determine what principles to include in the first awareness programme.

The financial organisation also required specific information in terms of ethical conduct, trust and change management. This information was necessary to aid management in tailoring their awareness programme to address any concerns in these areas. For instance, if management trusts its employees and the employees trust management, it is easier to implement new procedures and guide employees through changes of behaviour regarding information security. The perceptions of employees and management with respect to mutual trust need to be positive and should be regarded as a characteristic of the organisation that will aid in cultivating an information security culture from within. The information security culture questionnaire of Martins & Eloff focuses on these aspects and was found to be applicable to the requirements of the financial organisation. Apart from the data required by the researchers for the factor and reliability analysis, the financial organisation required the results of the survey for input to its awareness programme.

The information security culture questionnaire is divided into the following three sections (Martins 2002): (1) information security culture statements, (2) knowledge questions and (3) biographical questions.

Information security culture statements

This section assesses the perceptions of employees about eight different dimensions of information security: policies, management, programme, leadership, asset management, user management, change management and trust. A Likert scale (strongly agree, agree, unsure, disagree and strongly disagree) is used to answer the statements.

The following list reflects the statements in the information security asset management dimension:

- The organisation protects its information assets adequately (for example, systems and information).
- It is important to understand the threats to the information assets (for example, systems and information) in my department.
- Threats to security of information assets (for example, information and systems) are controlled adequately in my department.
- Information security is necessary in my department.
- The information assets (for example, systems and information) I work with need to be secured, either physically or electronically.
- I believe my business unit will survive if there is a disaster resulting in the loss of systems, people and/or premises.
- I feel safe in the environment I work in.
- I believe that the information I work with is adequately protected.

Knowledge questions

A section of knowledge questions is included to determine how much knowledge employees have about information security, and whether a low information security culture results from an educational problem or from perceptual concerns. A 'Yes/No' scale is used to answer these questions. The following five examples of knowledge questions are included in the information security culture questionnaire:

- The organisation has a written information security policy.
- I have read the information security policy sections that are applicable to my job.
- I know where to get a copy of the information security policy.
- I know what information security is.
- I know what an information security incident is.

Biographical questions

Biographical questions are included in the information security culture questionnaire in order to segment the data and draw comparisons within the population, for instance with regard to job levels or departments, as indicated by the following question:

What is your job level?

- Executive and senior managers
- Department managers and supervisors
- Operational staff (administrative, clerical, sales, etc.)
- Technology staff.

SURVEY METHODOLOGY

The survey methodology serves as a method that organisations can use to study information security behavioural content in general, as well as the attitude and opinions (Berry & Houston 1993) of employees with respect to information security in particular. This method is used to systematically gather data from members of an organisation for a specific purpose (Kraut 1996).

The process of designing, implementing, administering and reporting back on survey data is key to the success of the survey and perhaps even more important than the actual results generated (Kraut 1996). According to Berry & Houston (1993) and Kraut (1996), the main phases of a survey methodology should include planning and preparation, survey administration, data analysis, report writing and feedback to management and employees. Planning and preparation involve the participation of stakeholders, the customisation of the questionnaire, decisions on the population and sample size and a pilot study (Berry & Houston 1993; Church & Waclawski 1998). During the administration of the survey, the survey is communicated to the population and responses are monitored. The data are then statistically analysed, whereafter the report is compiled and feedback sessions are held to discuss action plans (Church & Waclawski 1998).

The following section discusses the survey methodology by illustrating how it was implemented in the financial organisation in order to obtain the data required for the factor and reliability analysis.

Planning and preparation

The first step in conducting a survey is to plan it (Berry & Houston 1993). The information security culture survey in the financial organisation was initiated through a formal project introduction meeting to obtain buy-in from relevant stakeholders and to discuss the project plan of operations (Berry & Houston 1993). As part of this meeting, the concept of information security culture was discussed, as well as the

approach that would be followed in conducting the survey. The stakeholders involved consisted of representatives from various departments – IT, information security, governance, risk management, human resources and training. The project sponsor was the Information Security Officer (ISO), and the various stakeholders assisted with the survey communication, technology set-up and coordination of the project across the target population to ensure that the required responses were obtained.

The second step was to conduct a workshop with the organisation's project team so as to customise the questionnaire (Berry & Houston 1993) developed by Martins (2002). IT as well as business representatives participated. Organisation-specific terminology was added to the information security culture questionnaire statements. The knowledge section of the information security culture questionnaire was also adjusted to incorporate questions specific to the environment of the organisation and any security awareness initiatives undertaken in the past. For instance, since the organisation has not rolled out an information security awareness programme in the past, no questions pertaining to such a programme were asked. The biographical questions were finalised based on the selected target population. These questions covered the business areas, geographical areas, length of service and job levels with respect to the organisation. It was decided that the information security culture questionnaire would be sent out to all employees in the selected business areas, altogether 12 572 employees. This method is referred to as convenience sampling (Brewton & Millward 2001).

Before the information security culture questionnaire could be rolled out to the target population, it had to be pretested on a small sample of employees to allow the researcher to understand the anticipated reactions of the larger group and to revise or restructure questions where necessary (Berry & Houston 1993). A group of 20 employees in the organisation completed the pilot survey in order to test the face validity of the information security culture questionnaire. Face validity is concerned with whether the questionnaire assesses what it says it does on the 'face of it' (Furnham & Gunter 1993). Minor adjustments were made to some of the culture statements to ensure that all employees would interpret the statements in the same manner. For instance, examples were added to some terms, and the word 'department' was changed to 'business area' as indicated in the box.

> My *business area* protects its information assets adequately *(e.g. systems and information in electronic or paper format)*.

The survey tool, Survey Tracker (2005), was used as the survey software to distribute, capture and conduct the survey analysis (Berry & Houston 1993). The information security culture questionnaire that was signed-off by the ISO had been designed in HTML format in Survey Tracker according to the scientific rules of

scales and question types built into the software. In collaboration with the IT department, a link to the information security culture questionnaire was added to the organisation's Intranet site, where employees could complete it. Figure 1 is an example of two statements extracted from the HTML-designed information security culture questionnaire.

	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
14. Information security should be part of key performance measures for the employees of the Group	•	•	•	•	•
15. Employees should be monitored on their compliance to information security policies and procedures (e.g. measuring the use of e-mail, monitoring which sites an individual visits or what software is installed on personal computes).	•	•	•	•	•

Figure 1: Extract from information security culture questionnaire

Survey administration

Communicating the survey and its objectives to employees is crucial in order to enhance the response rate and the quality thereof (Dillon, Madden & Firtle 1993). If questions are of a sensitive nature, and employees wish to remain anonymous, the organisation must ensure that individual responses cannot be identified (Berry & Houston 1993). For the purpose of this survey, the responses of the completed information security culture questionnaires were automatically saved in a file on one of the organisation's secure servers.

A communication e-mail was sent out to all employees from the 'Communication' mailbox a week before the survey was launched to prepare them for and inform them of the forthcoming survey. The survey ran for four weeks, during which employees were continually encouraged to complete the information security culture questionnaire online.

During this period, the responses were tracked to ensure that a statistically representative response was obtained for each biographical area into which the data would be segmented. Table 1 provides a summary of the divisions of the organisation, the number of employees in each, the statistically representative sample required and the actual response obtained. The method designed by Krejcie & Daryle (1970) was used to determine the required sample size. In only four divisions was this not representative. Trends were considered for these divisions.

When a validity test is conducted, the commonly accepted criterion is to have at least 100 respondents, or five times the number of responses compared to the number

of questions in the questionnaire (Martins 2000). The more accepted criterion is to have at least ten times the number of responses. This will ensure that the conclusions drawn from the sample data are not sample specific and that it is possible to generalise the findings (Martins 2000). The information security culture questionnaire consists of 42 statements that were used in the factor and reliability analysis. Overall, a representative number of 4 735 employees participated in the survey, which was a more than adequate sample.

Table 1: Information security culture questionnaire – representative sample

Division/ Business unit	Total number of employees	Sample required based on Krejcie & Daryle method	Actual responses	Representative (Yes/No)
Division A	1 847	318	1 213	Yes
Division B	261	155	160	Yes
Division C	1 146	217	500	Yes
Division D	132	75	93	Yes
Division E	3 481	346	675	Yes
Division F	668	191	381	Yes
Division G	1 311	224	536	Yes
Division H	311	172	124	No
Division I	660	245	209	No
Division J	72	61	42	No
Division K	77	64	40	No
Division L	2 606	335	545	Yes
Division M	No data	No data	144	No data
No response	n/a	n/a	73	n/a
Overall	12 572	355	4 735	Yes

Statistical analysis and results of the survey

The survey results were analysed using Survey Tracker (2005). Figure 2 shows the job levels of respondents. The respondents represented all job levels in the organisation: executive and senior managers (3.97%), department managers and supervisors (21.94%), operational job staff (64.16%) and technology staff (8.51%). Most respondents had worked for the organisation for more than ten years (32.06%) or for between 5 and ten years (23.59%), 77.4% worked at head office, and the rest at

branch offices. Responses were received from all nine provinces in South Africa, with the majority from Gauteng (62.09%), followed by the Western Cape (12.61%) and KwaZulu Natal (9.17%).

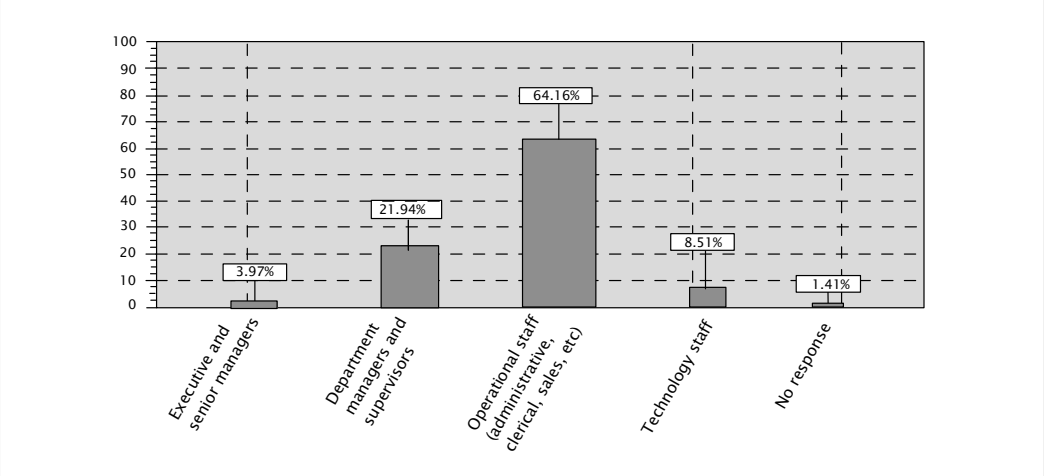

Figure 2: Job levels of respondents

Figure 3 shows the results of three of the knowledge questions as an example. The first column lists the question, the second provides the number of people that responded to the question, and the last column gives the percentage of people that answered 'Yes'. The figure illustrates that only 70.2% of the 4 691 respondents that answered the last question know where to get a copy of the information security policy. This would indicate that the organisation needs to communicate to employees where to obtain a copy of the information security policy and to ensure that the policy is kept or saved in a location where it is easy for employees to access it.

Statements	Count	Percentages of 'Yes' responses 0 20 40 60 80 100
The organisation has a written information security policy.	4 584	94.9%
I know what information security is.	4 690	92.2%
I know where to get a copy of the information security policy.	4 691	70.2%

Figure 3: Knowledge statement results

This concludes the discussion pertaining to the survey methodology used to conduct the information security culture assessment in the financial organisation in order to obtain data that could be used to validate the information security culture questionnaire.

FACTOR AND RELIABILITY ANALYSIS

The concept of validity implies that the researcher must ensure that the questionnaire assesses what it claims to assess (Berry & Houston 1993; Dillon, Madden & Firtle 1993; Furnham & Gunter 1993). Over time, such a questionnaire will yield reliable and stable results that prove to be valid (Dillon, Madden & Firtle 1993). Construct validity is considered for the validity analysis of the information security culture questionnaire. Construct validity is established using the principle components factor analysis to assess the robustness of the questionnaire dimensions, thereby identifying clusters of questions (statements) and forming new dimensions (Brewerton & Millward 2001). In the industrial psychology literature and in research, factor analysis is frequently used to assess whether instruments (questionnaires) measure substantive constructs which in this case are the nine dimensions of the information security culture questionnaire. Factor analysis as a statistical technique is employed to determine or uncover any underlying 'structure' that may exist in a data set (Brewton & Millward 2001; Howell 1995). It has various applications, which include establishing the structure of 'traits' that underlie personality, understanding the relationship between various performance criteria, and exploring the relationship between established work-related constructs (for example, leadership, communication, governance, awareness) (Brewton & Millward 2001; Martins & Von der Ohe 2003).

The principal components factor analysis (PCA) is a data analysis tool that is generally used to reduce the dimensionality (number of questions or statements) of a large number of interrelated questions, while retaining as much of the information (variation) as possible (Hintze 1997). The Number Cruncher Statistical Software (NCSS) program (Hintze 1997) was used for this purpose.

The latent root criterion (Hair, Anderson, Tatham & Black 1995), which specifies that all factors with eigenvalues of 1.00 or greater should be retained, was used. The eigenvalues are helpful in determining the variance of each factor and thus how many factors should be retained. The use of the eigenvalue as a cut-off point is possibly the most reliable criterion in determining how many factors to retain. All factors with a factor value greater than 1.00 were retained (Hintze 1997).

An initial factor extraction was done according to PCA, and the inter-correlation matrix was rotated according to the varimax method using the NCSS tool. The varimax method is used to obtain new factors or dimensions that are each highly correlated with only a few of the original variables (Hintze 1997).

Next, the reliability of each factor was determined by means of an item analysis (Cronbach alpha) that examines the correlation between each item and the scale total within a sample (Brewerton & Millward 2001). An item analysis is used to examine the frequencies and descriptive statistics for each item on the survey across all responses obtained (Church & Waclawski 1998). Reliability testing (Brewerton &

Millward 2001) is concerned with the degree of data consistency across a defined dimension. The purpose of both these techniques is to determine the reliability of an instrument (questionnaire). Both techniques were employed to assess whether the security culture instrument measures the substantive constructs (dimensions) and to test the reliability thereof.

DISCUSSION

The variance rotation isolated four factors, as listed in Table 2, which could be used as the four new information security culture dimensions and which accounted for 53.3% of the variance. According to Hintze (1997), factors that account for at least 50% of the variance are accepted. The interpretation of the factor matrix showed that none of the statements had a factor loading lower than 0.30, which is regarded as the cut-off point. According to Hair et al. (1995) a factor loading above 0.30 is regarded as meaningful and can be included in the dimensions. The internal consistency of the four new dimensions varies between 0.955795 and 0.676533 (Table 3). According to Brewton & Millward (2001), internal reliabilities between 0.6 and 0.7 are generally accepted as an absolute minimum to be identified as a factor.

Table 2: Results of initial factor analysis

Factor	Statement numbers
Factor 1	14, 15, 16, 22, 25*, 26, 28, 30, 33, 35, 38, 39, 40, 41, 42, 43, 44, 46, 47, 48, 49, 51, 52, 53
Factor 2	12, 17, 21, 23, 24, 25, 27, 28, 29, 31, 34, 36, 37
Factor 3	13, 18, 19, 22
Factor 4	45, 49, 50

* Item 25 loads high on factors 1 and 2

Table 3: Reliability analyses of initial analysis

Factors	Cronbach alpha	Number of items/ statements	Comments
Factor 1	0.955795	24	Item 25 loads high on factors 1 and 2
Factor 2: Management of information security	0.890352	16	
Factor 3: Performance management	0.677747	4	Item 22 loads high on factors 1 and 3
Factor 4: Performance accountability	0.676533	3	

A second-phase factor analysis was conducted for factor 1 in order to determine whether sub-dimensions could be formed. The same techniques and criteria were used as with the first analysis. The factors and factor loadings are presented in Tables 4 and 5. The factor loadings range between 0.807570 and 0.933200.

Table 4: Results of the factor analysis for the second-phase analysis – Factor 1

Factor	Statement numbers
Factor 5: Communication	22, 33, 35
Factor 6: Governance	14, 15, 16, 20, 25, 26, 30
Factor 7: Capability development	38, 39, 40, 41, 42, 43, 44, 46, 47, 48, 49, 51, 52, 53

Table 5: Reliability analysis of second-phase analysis

Factors	Cronbach Alpha	Number of items
Factor 5: Communication	0.807570	3
Factor 6: Governance	0.891884	7
Factor 7: Capability development	0.933200	14

Naming of factors

Conceptual naming of factors 2 to 7 was done after detailed inspection of the individual items (statements). The purpose was to attach a dimension name to each factor to make it understandable and identifiable for the information security culture questionnaire. Each of the new information security culture dimensions will next be discussed briefly.

Management of information security (factor 2)

This dimension includes the applicability of the information security policy, the understanding of threats to information assets, a willingness to change working practices to ensure the security of information assets and an acceptance of a responsibility towards information security.

Performance management (factor 3)

The items included in this dimension determine whether information security should be part of key performance measures, whether employees believe that they should be monitored, and whether the contents of the information security policy had been effectively explained to them, thus enabling employees to adhere to the policy.

Performance accountability (factor 4)

This dimension focuses on aspects such as whether action should be taken against people that do not adhere to the information security policy, whether employees feel safe where they work and whether people should be held accountable for their actions if they do not adhere to the information security policy.

Communication (factor 5)

The items included in this dimension focus on aspects such as the explanation of the information security policy, informing employees in a timely manner how information security changes will affect them, and informing people about what is expected of them regarding information security.

Governance (factor 6)

This factor focuses on aspects such as whether management adheres to the information security policy, the adequate protection of information assets, the perception of the importance of information security, and adequate control over information security assets.

Capability development (factor 7)

This dimension focuses on a number of aspects relating to employee trust, the commitment of time to information security, adherence to the information security policy by the various business areas, commitment to the policy and a belief that information is adequately protected.

This questionnaire with the six revised dimensions is hereafter referred to as the Information Security Culture Assessment (ISCA) questionnaire. Table 6 details the eight dimensions of the original information security culture questionnaire compared with the six new dimensions of the ISCA, as well as the number of statements per dimension. The six new dimensions have been constructed on the basis of the factor and reliability analysis as discussed, thereby ensuring that the new information security culture questionnaire meets the requirements for a reliable questionnaire as accepted in the statistical field.

After an analysis had been conducted of each of the items (statements) in the six ISCA dimensions, the items were regrouped and applicable names were given to each group of items relating to a single concept. The individual statements were left unchanged. Figure 4 illustrates the composition of the dimensions and groups the items into the identified concepts that are measured in each dimension.

For example, the management of the information security dimension involves four main concepts that are measured, namely accepting ownership, accepting change,

Table 6: Comparing the old and revised information security culture dimensions

Old information security culture questionnaire dimensions (factors)	Number of statements per dimension (factors)	New information security culture dimensions (factors) of ISCA	Number of statements per dimension (factors)
Information security policies	2	Management of information security	12
Information security management	2	Performance management	4
Information security programme	7	Performance accountability	3
Information security leadership	8	Communication	3
Information asset management	8	Governance	7
User management	8	Capability development	14
Change management	4		
Trust	3		
Total number of items	**42**	**Total number of items**	**43**

necessity of resources and understanding threats. The items (statements) in the information security culture questionnaire will determine users' perceptions with regard to each of the four concepts.

Table 7 outlines the statements of the revised governance dimension (previously the information assets management dimension) in order to illustrate how the statements were regrouped on the basis of the factor analysis.

CONCLUSION AND RECOMMENDATIONS

The paper addressed its purpose by validating an information security culture questionnaire. This was enabled by conducting an information security culture assessment in a financial organisation and using the data to perform a factor and reliability analysis. As output, a revised information security culture questionnaire is proposed that yields reliable results should it be used to assess information security in other organisations or as a follow-up assessment in the financial institution to benchmark the results.

In the light of the research results, it is evident that there are revised or possible additional dimensions that could be constructed for the information security culture questionnaire. Based on the assessment that was conducted, as well as other organi-

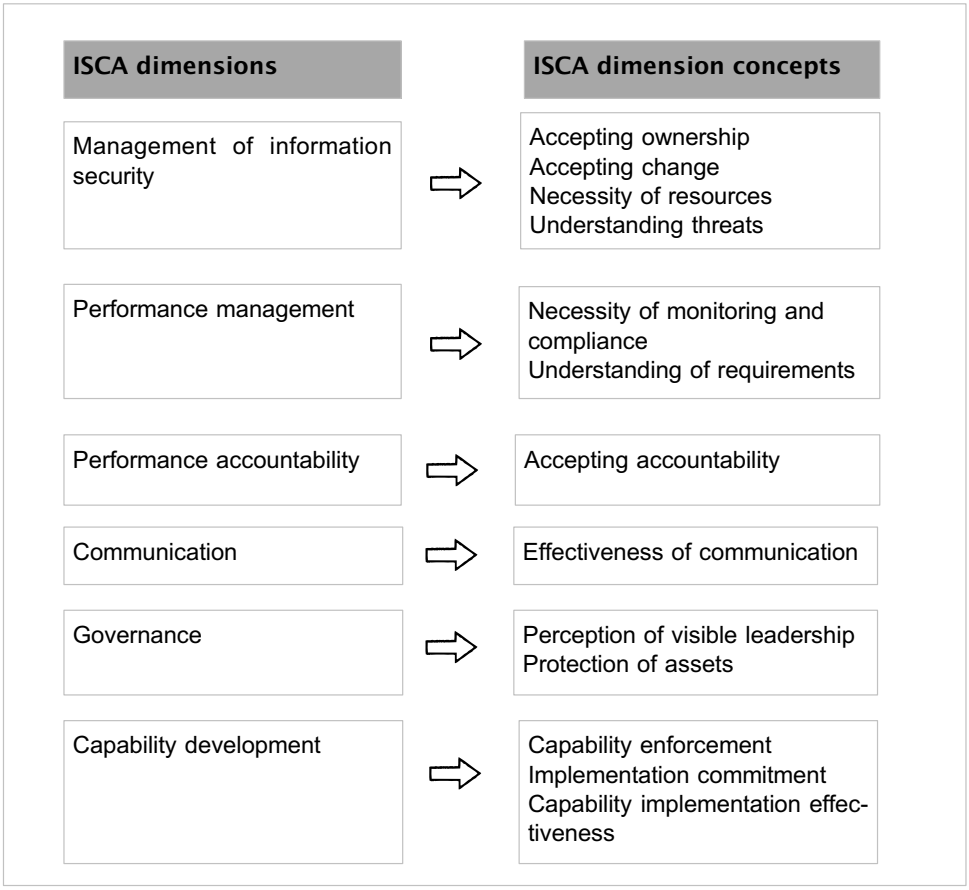

Figure 4: ISCA dimensions and concepts

Table 7: Governance dimension statements

Governance concepts	**Governance dimension statements (items)**
Perception of visible leadership	1 Management in my department **adheres** to the information security policy.
	2 Department managers and supervisors perceive information security as **important**.
	3 Executive and senior management perceive information as **important**.
	4 Information security is perceived as **important in** my business area.
	5 The staff in our department perceive information security (e.g. sharing confidential information) as **important**.
Protection of assets	6 My business area **protects** its information assets adequately.
	7 Threats to security of information assets are **adequately controlled** in my department.

sations where the information security culture assessment was conducted, it was determined that certain aspects of the information security culture questionnaire could be further enhanced to meet the needs of the industry. The following should be considered when further enhancing ISCA:

- The dimension on user knowledge and awareness could be enhanced to enable more in-depth correlations to the culture statements.
- Attention should be focused on ethical considerations and the perception of users with regard to sensitive information.
- More attention should be focused on communication in terms of what the preferred channels are and how effective employees perceive them to be.
- The performance measurement, performance accountability and communication dimensions of ISCA could be expanded to include at least three to five statements per dimension (Church & Waclawski 1998).
- The completeness of the regrouped statements in the new dimensions should be investigated. For example, the governance dimension should be assessed to identify all concepts of governance that pertain to an information security culture in order to ensure the completeness of the statements in each ISCA dimension.

REFERENCES

Abu-Musa, A.A. 2003. 'The perceived threats to the security of computerized accounting information systems', *Journal of American Academy of Business,* 3(1/2): 9–20.

Baggett, W.O. 2003. 'Creating a culture of security', *Internal Auditor*, 60(3): 37–41.

Berry, M.L. & Houston, J.P. 1993. *Psychology at Work*. Winsconsin: Brown and Benchmark.

Bresz, F.P. 2004. 'People – Often the weakest link in security, but one of the best places to start', *Journal of Health Care Compliance*, 6(4): 57–60.

Brewton, P. & Millward, L. 2001. *Organizational Research Methods*. London: Sage.

Church, A.H. & Waclawski, J. 1998. *Organizational Surveys – a Seven Step Approach*. San Francisco, CA: Jossey-Bass.

CITEC. 2005. 'Building a strong security culture'. [Online] Available at: www.citec.com.au/news/featureNews/2005/April/security_culture.shtml. Accessed: January 2006.

COBIT (Control Objectives for Information and related Technology). 2004. *COBIT Security Baseline – An Information Security Survival Kit*. USA: IT Governance Institute.

Dervin, L., Kruger, H. & Steyn, T. 2006. 'Value-focused assessment of information communication and technology security awareness in an academic enviornment', *Security and Privacy in Dynamic Environments*, pp 448–453. IFIP International Federation for Information Processing, 201.

Dillon, W.R., Madden, T.J. & Firtle, N.H. 1993. *Essentials of Marketing Research*. Boston: Irwin.

Furnham, A. & Gunter, B. 1993. *Corporate Assessment: Auditing a Company's Personality*. London: Routledge.

Gaunt, N. 2000. 'Practical approaches to creating a security culture', *International Journal of Medical Informatics*, 60(2): 151–157.

Hair, J.F., Anderson, R.E., Tatham, R.L. & Black, W.C. 1995. *Multivariate Data Analysis with Readings*, 4th edition. Englewood Cliffs, NJ: Prentice Hall.

Hintze, J.L. 1997. *Number Cruncher Statistical Systems,* version 5.03 5/90. Kaysville, UT: NCSS.

Howell, D.C. 1995. *Fundamental Statistics for the Behavioral Sciences,* 3rd edition. International Standards Organisation. [Online] Available at: www.iso.ch. Accessed: January 2005.

ISF (Information Security Forum). 2000. *Information Security Culture – A Preliminary Investigation*. United Kingdom: ISF.

ISO. 2005. Information technology. Security techniques. Code of practice for information security management. ISO/IEC 17799 (BS 7799–1: 2005).

Kraut, A.I. 1996. *Organizational Surveys*. San Francisco, CA: Jossey-Bass.

Krejcie, R.V. & Daryle, M.W. 1970. 'Determining sample size for research activities', *Educational and Psychological Measurement*, 30.

Martins, A. 2002. 'Information security culture', MCom dissertation, Rand Afrikaans University, Johannesburg.

Martins, E.C. 2000. 'Die invloed van organisasiekultuur op kreatiwiteit en innovasie in 'n universiteitbiblioteek', MCom dissertation, University of South Africa, Pretoria.

Martins, A. & Eloff, J.H.P. 2002. 'Information security culture', *Security in the Information Society,* pp. 203–214. IFIP/SEC2002. Boston, MA: Kluwer Academic Publishers.

Martins, N. & Von der Ohe, H. 2003. 'Organisational climate measurement – new and emerging dimensions during a period of transformation', *South African Journal of Labour Relations,* (27)3 & 4: 41–59.

PWC (PricewaterhouseCoopers). 2004. Information Security Breaches Survey. [Online] Available at: www.dti.gov.uk/industry_files/pdf/isbs_2004v3.pdf. Accessed: January 2005.

Robbins, S. 2001. *Organizational Behaviour,* 9th edition. New Jersey: Prentice Hall.

Robbins, S., Odendaal, A. & Roodt, G. 2003. *Organisational Behaviour – Global and Southern African Perspectives*. Cape Town: Pearson Education.

Ruighaver, A.B. & Maynard, S.B. 2006. 'Organisational security culture: More than just an end user phenomenon', *Security and Privacy in Dynamic Environments*, pp 425–430, IFIP International Federation for Information Processing, 201.

Schein, E.H. 1985. *Organizational Culture and Leadership*. San Francisco, CA: Jossey-Bass.

Schlienger, T. & Teufel, S. 2002. 'Information security culture', *Security in the Information Society*, pp 191–201. IFIP/SEC2002. Boston, MA: Kluwer Academic.

Schlienger, T. & Teufel, S. 2003. 'Analysing information security culture: Increased trust by an appropriate information security culture', Paper presented at International Workshop on Trust and Privacy in Digital Business Trust in conjunction with 14th International Conference on Database and Expert Systems Applications, Prague, Czech Republic.

Schlienger, T. & Teufel, S. 2005. 'Tool supported management of information security culture', Paper presented at 20th IFIP International Information Security Conference, Makuhari-Messe, Chiba, Japan.

Stewart, J.N. 2006. 'CSO to CSO: Establishing the security culture begins at the top'. [Online] Availabe at: cisco.com/web/about/security/intelligence/05_07_securityculture.html. Accessed: January 2006.

Survey Tracker. 2005. [Online] Available at: www.surveytracker.com. Accesed: January 2005.

Tessem, M.H. & Skaraas, K.R. 2005. 'Creating a security culture'. [Online] Availabe at: www.telenor.com/telektronikk/volumes/pdf/1.2005/Page_015–022.pdf. Accessed: January 2006.

OECD (Organisation for Economic Cooperation and Development). 2005. 'The promotion of a culture of security for information systems and networks in OECD countries (OECD)', DSTI/ICCP/REG(2005)1/FINAL.2005. [Online] Available at: www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html. Accessed: August 2006.

Thomson, I. 2004. 'IT security culture must start from the top Global survey warns senior execs against "delegating" security awareness'. [Online] Availalbe at: www.vnunet.com/vnunet/news/2125904/securityculturestarttop. Accessed: January 2006.

Von Solms, B. 2000. 'Information security – the third wave?' *Computers and Security*, 19(7): 615–620.

Von Solms, B. 2006. 'Information security – the fourth wave', *Computers and Security,* 25 (2006): 165–168.

Zakaria, O. 2006. 'Internalisation of information security culture amongst employees through basis security knowledge', *Security and Privacy in Dynamic Environments*, pp 437–441. IFIP International Federation for Information Processing, 201.

APPENDIX E – PAPER PUBLISHED IN JOURNAL: AN INFORMATION SECURITY GOVERNANCE FRAMEWORK

Information Systems Management, 24:361–372, 20
Copyright © Taylor & Francis Group, LLC
ISSN: 1058-0530 print/1934-8703 online
DOI: 10.1080/10580530701586136

Taylor & Francis
Taylor & Francis Group

An Information Security Governance Framework

A. Da Veiga
PhD Student,
University of Pretoria,
South Africa.

J. H. P. Eloff
Head of Department and
Professor of Computer Science,
Department of Computer Science,
University of Pretoria,
South Africa.

ABSTRACT Information security culture develops in an organization due to certain actions taken by the organization. Management implements information security components, such as policies and technical security measures with which employees interact and that they include in their working procedures. Employees develop certain perceptions and exhibit behavior, such as the reporting of security incidents or sharing of passwords, which could either contribute or be a threat to the securing of information assets. To inculcate an acceptable level of information security culture, the organization must govern information security effectively by implementing all the required information security components. This article evaluates four approaches towards information security governance frameworks in order to arrive at a complete list of information security components. The information security components are used to compile a new comprehensive Information Security Governance framework. The proposed governance framework can be used by organizations to ensure they are governing information security from a holistic perspective, thereby minimising risk and cultivating an acceptable level of information security culture.

KEYWORDS information security governance framework, information security components, information security culture, information security behavior

INTRODUCTION

Information security encompasses technology, processes, and people. Technical measures such as passwords, biometrics, and firewalls alone are not sufficient in mitigating threats to information. A combination of measures is required to secure systems and protect information against harm. Processes such as user registration and de-registration and people aspects such as compliance, training and leading by example need to be considered when deploying information security. As the deployment of information security evolved, the focus has been shifting towards a people-orientated and governance-orientated approach.

The so-called first phase of information security was characterised by a very technical approach in securing the IT environment. As time went by, the "technical people" in organizations started to realize that management played a significant role in information security and that top management

Address correspondence to
A. Da Veiga,
PO Box 741, Glenvista,
Johannesburg, 20098, South Africa.
E-mail: adele.daveiga@kpmg.co.za

needed to become involved in it too (2000). This led to a second phase, where information security was incorporated into organizational structures. These two phases, namely technical protection mechanisms and management involvement have since continued in parallel. Organizations came to realize that there were other elements of information security that had been disregarded in the past. They concluded that the human element, which poses the greatest information security threat to any organization, urgently needs to be addressed (Da Veiga, Martins, & Eloff, 2007; Von Solms, 2000, 1997) and more attention be given to the information security culture within organizations (Von Solms, 2000). This third phase of information security emphasizes that information security should be incorporated into the everyday practices performed as part of an employee's job to make it a way of life and so cultivate an effective information security culture throughout the organization. An information security culture is defined as the assumption about those perceptions and attitudes that are accepted and encouraged in order to incorporate information security characteristics as the way in which things are done in an organization (Martins & Eloff, 2002).

According to the Cobit Security Baseline (2004), executives are responsible for communicating the right information security culture and control framework and for exhibiting acceptable information security behavior. This relates to the fourth phase of information security, namely the development and role of information security governance (Von Solms, 2006). Information security governance can be described as the overall manner in which information security is deployed to mitigate risks.

One of the key drivers in the fourth phase is the prevention of risks such as fraud and social engineering. The Information Security Breaches Survey conducted by PriceWaterhouseCoopers (PWC, 2004) stated that the number of technology-related security incidents such as system failures or data corruptions organization experience is very high, but that "human error rather than flawed technology is the root cause of most security breaches" (PWC, 2004). According to PriceWaterhouseCoopers, the solution would be to create a security-aware culture. Management is starting to realize that human interaction with technical controls could lead to serious fraud or social engineering. Von Solms (2006), consequently emphasises that good information security governance is essential to address these risks.

The risks faced by the organization can only be addressed when a governance framework for information security is in place and equipped with specific controls that executives may use to direct employee behavior. Such a governance framework can enable organizations to make provisions for human behavior in their information security initiatives, in order to cultivate an acceptable level of information security culture. In other words, there is a need for an information security governance framework that considers the technical and procedural controls of the past, but that also takes human behavior into account. Such a framework can be utilized to cultivate the acceptable level of information security culture in order to minimize risks posed to information assets.

The purpose of this article is to evaluate four current approaches towards information security governance frameworks in order to construct a new comprehensive Information Security Governance framework. This new Information Security Governance framework considers technical, procedural and human behavioral components to provide an all-encompassing and single point of reference for governing information security. The four approaches that are evaluated in the following section are ISO 17799 (2005), PROTECT (Eloff & Eloff, 2005), the Capability Maturity Model (McCarthy & Campbell, 2001), and the Information Security Architecture (ISA) (Tudor, 2000). The third section provides a comprehensive list of information security components based on the components of the four mentioned approaches. The information security components are used to construct the Information Security Governance framework (see Figure 1). Finally, the Information Security Governance framework is proposed and discussed in the last section.

INFORMATION SECURITY GOVERNANCE FRAMEWORKS—EXISTING APPROACHES

Information security behavior could be explained by illustrating the security we implement in our

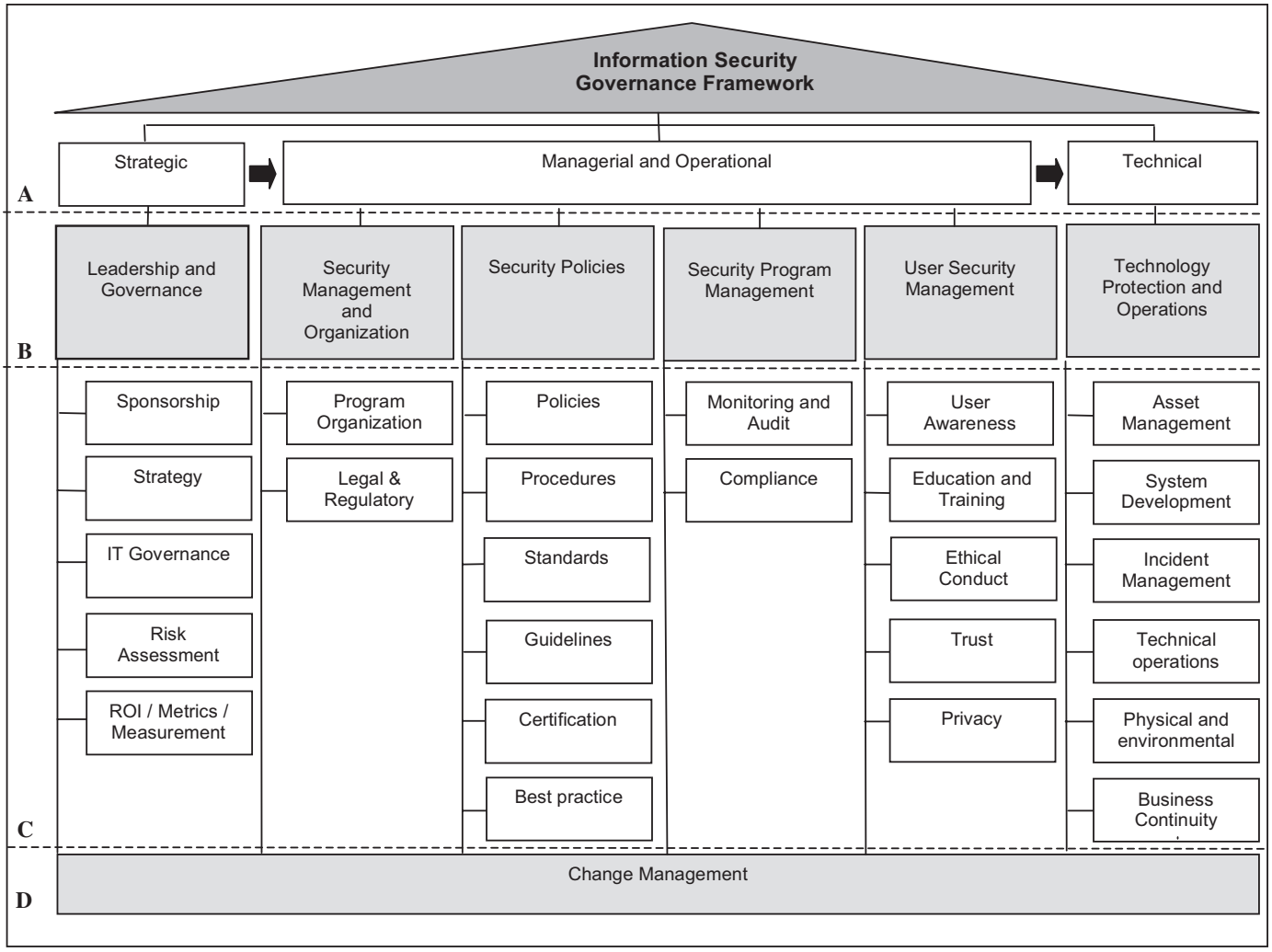

FIGURE 1 **Information Security Governance framework.**

houses. A homeowner could implement burglar proofing at each window, but upon leaving the house leave the front door unlocked. The security measures are therefore ineffective due to his behavior. In the same way, organizations implement security controls such as anti-virus programs, firewalls, and passwords. There is no sense in implementing these controls if users share passwords and connect through dialup to the Internet, bypassing the firewall.

The behavior of employees needs to be directed and monitored to ensure compliance with security requirements. As such, management needs to implement and communicate specific security controls—also referred to as components (Tudor, 2000; ISO 17799, 2005) —before they can expect employees to adhere to and exhibit an acceptable level of information security culture.

Various researchers and organizations have defined the components of information security and how an organization should go about implementing them (ISO 17799, 2005; Tudor, 2000; McCarthy & Campbell, 2001; Teufel, 2003). Information security components can be described as the principles that enable the implementation and maintenance of information security—such as an information security policy, risk assessments, technical controls, and information security awareness. These components can be encompassed in an information security governance framework where the relationship between the components is illustrated. The Information Security Governance framework provides organizations with an understanding of the requirements for a holistic plan for information security. It also combines technical, procedural, and people-orientated components for the purpose of cultivating an

appropriate level of information security minimising risks posed to information assets.

The subsequent sections provide a description of four current approaches to information security governance frameworks in order to define and construct a comprehensive new Information Security Governance framework (Figure 2).

ISO/IEC 177995 and ISO/IEC 27001

The Information Technology Security techniques—Code of Practice for Information Security Management (ISO/IEC 17799, 2005) of the Information Security Organization (ISO) take the form of guidance and recommendations and are intended to serve as a single reference point for identifying the range of controls needed for most situations where information systems are used. ISO/IEC 17799 (2005) has gradually gained recognition as an essential standard for information security (ISO/IEC, 2005). It consists of the 11 control sections detailed in Table 1.

The certification standard ISO 27001 (2005) is regarded as part two of ISO/IEC 17799 (2005) and proposes an approach of continuous improvement through a process of establishing, implementing, operating, monitoring, reviewing, maintaining and improving the organization's information security management system (ISO, 2005; IEC, 2005). The previously mentioned international standards are considered as a single encompassing approach since ISO/IEC 17799 (2005) details the components of information security and ISO/IEC 27001 (2005) outlines the approach aimed at implementing and managing them.

PROTECT

The research conducted by Eloff and Eloff (2005) introduced a comprehensive approach towards information security, namely PROTECT. This is an acronym for Policies, Risks, Objectives, Technology, Execute, Compliance, and Team. PROTECT is aimed at addressing all aspects of information security. It involves an approach that considers various and well-integrated controls in order to minimize risk and ensure effectiveness and efficiency in the

ntrol Sections of ISO/IEC 17799
(Adapted from ISO/IEC 17799, 2005)

1. **Security policy** that aims to provide management direction and support for information security, including laws and regulations.
2. **Organization of information security** that constitutes the process implemented to manage information security within the organization.
3. **Asset management** that focuses on asset inventories, information classification, and labeling.
4. **Human resources** security that considers permanent, contractor, and third-party user responsibilities to reduce the risk of theft, fraud, and misuse of facilities. This section also includes awareness, training, and education of employees.
5. **Physical and environmental** security controls that allow only authorized access to facilities and secure areas.
6. **Communications and operations management** that focus on the correct and secure operation of information-processing facilities, such as segregation of duties, change management, malicious code, and network security.
7. **Access controls** that manage user access to information and include clear desk principles, network access controls, operating system access controls, passwords, and teleworking.
8. Information **systems acquisition, development, and maintenance** that ensure the security of user-developed and off-the-shelf products.
9. Information security **incident management** that ensures that incidents are communicated in a timely manner and that corrective action is taken.
10. **Business continuity management** that focuses on business continuity plans and the testing thereof.
11. **Compliance** in terms of statutory, regulatory or contractual, laws, audit and organizational policy requirements, or obligations.

organization. The seven control components of PROTECT are aimed at implementing and managing an effective information security program from a technology perspective as well as a people perspective and are summarised in Table 2.

Capability Maturity Model

The Capability Maturity Model (McCarthy & Campbell, 2001) approach provides a set of security controls used to protect information assets against unauthorised access, modification or destruction. The model is based on a holistic view of information security and encompasses seven main control levels as portrayed in Table 3.

TABLE 2 Control Components of PROTECT (Adapted from Eloff & Eloff, 2005)

1 The **policy** component includes information security policies, procedures, and standards, as well as guidelines for maintaining these.
2 **Risk** methodologies such as CRAMM and Octave, as well as automated tools to identify system vulnerabilities are covered in the risk component.
3 **Objective** refers to the main objective of PROTECT, namely to minimize risk exposure by maximizing security through the implementation and monitoring of a comprehensive set of controls.
4 **Technology** refers to hardware, software, and systems product components of the IT infrastructure and, where possible, the use of certified products.
5 Information security controls need to be established, maintained, and managed. **Execute,** therefore, refers to a proper information security management system environment.
6 The **compliance** component covers both internal compliance with the organization's policies and external compliance with information security expectations set by outside parties to the organization. Compliance also includes international codes of practice, legal requirements, and international standards.
7 **Team** refers to the human component, namely all the employees of the organization, where each has a responsibility towards securing information. The objective is to create a security-aware workforce that will contribute to an improved information security culture.

ntrols Levels of the Capability Maturity Model (Adapted from McCarthy & Campbell, 2001)

1 **Security leadership:** Security sponsorship/posture, security strategy, and return on investment/metrics.
2 **Security program**: Security program structure, security program resources, and skill sets.
3 **Security Policies**: Security policies, standards, and procedures.
4 **Security Management**: Security operations, security monitoring, and privacy.
5 **User Management**: User management and user awareness.
6 **Information Asset Security:** Application security, database/meta security, host security, internal and external network security, anti-virus, and system development.
7 **Technology Protection & Continuity**: Physical and environmental controls and continuity-planning controls.

The first level, security leadership, stresses the importance of an executive level security representative and an information security strategy. This should be the starting point for deploying both a long-term and short-term information security strategy within an organization. Next, a security program with defined roles and responsibilities for information security tasks should be developed and implemented. The roles of inter alia information security officer, network specialist, anti-virus specialist, database specialist, and Helpdesk personnel need to be defined. On the third level, security policies, standards, and guidelines need to be compiled to direct the implementation of information security. These policies, standards, and guidelines should cover the technical, procedural, and human aspects of information security. Security management will then form part of day-to-day operations, which include the monitoring of users and the technology deployed as directed by the previous layers. The organization subsequently needs to ensure that users are aware of policies and that user profiles are managed. Finally, the approach addresses information asset security that encompasses the technology aspects of information security, such as configuring a secure firewall, network and database. Technology protection comprises the last layer and focuses not only on the IT environment and its continuity, but also includes business continuity and disaster recovery.

The objective of the Capability Maturity Model approach is to start from the top on a strategic level and work down to the technology levels, guided by the direction provided by the strategic levels. In implementing information security, the model is used to assess the current information security capability and risks and to architect the appropriate solution to mitigate risks. The solution as well as monitoring capabilities are then implemented and integrated with current processes.

Information Security Architecture (ISA)

Tudor (2000) proposes a comprehensive and flexible Information Security Architecture (ISA) approach to protect an organization's assets against threats. This approach highlights five key principles, listed in Table 4, that are used to understand the risk environment in which organizations operate in order to evaluate and implement controls to mitigate such risks. There is also a focus on country regulations to ensure that each organization's confidential

TABLE 4 Principles of the Information Security (Adapted from Tudor, 2000)

1. **Security organization and infrastructure:** Roles and responsibilities are defined and executive sponsorship is established.
2. **Security policies, standards, and procedures**: Policies, standards and procedures are developed.
3. **Security program:** A security program is compiled taking risk management into account.
4. **Security culture awareness and training:** Users are trained and awareness is raised through various activities. Trust among users, management, and third parties are established.
5. **Monitoring compliance:** Internal and external monitoring of information security is conducted.

information is protected accordingly. The principles encompass aspects of process, as well as technology to address organizations' security needs.

The first principle relates to security organization and infrastructure with defined roles and responsibilities, as well as to executive sponsorship. The second principle requires that security policies, standards and procedures supported by management be developed and implemented. Security control requirements stated in the security policies cannot be deployed in isolation, but must be considered in terms of the risks the organization faces. Therefore, as a third principle, risk assessments must be performed across platforms, databases, applications, and networks, and a process should be instituted to provide an adequate budget for resources to address risks and implement controls. In order for the controls to operate effectively, users need to be made aware of their responsibility and encouraged to attend training programs. This fourth principle aims to establish an environment of trust among users, management and third parties to enable transactions and protect privacy. The fifth and last principle focuses on compliance testing and audits by internal and external auditors to monitor the effectiveness of the security program. The number of security incidents and Internet sites visited, as well as the levels of network and email usage constitutes aspects that must be monitored to allow a proactive approach towards addressing threats to information. In Tudor's latest research, aspects such as business continuity and disaster recovery are included as part of the approach aimed at preserving organizational information and assets (Holborn, 2005).

COMPREHENSIVE LIST OF INFORMATION SECURITY COMPONENTS

A comprehensive list of components was compiled from the relevant sections of ISO 17799, components of PROTECT, levels of the Capability Maturity Model and principles of the ISA approach. These components were selected from each approach where a component was depicted as a key principle (e.g., "risk focus"), or as an information security control (e.g., "business continuity"). Where components overlapped between approaches such as "policies," a combined component category was defined.

A comprehensive list of components is presented in Table 5. The objective of Table 5 is to consolidate the components of the various approaches as discussed in the previous paragraph. It also shows the % representation of each approach's components. This comprehensive list of components forms the basis of the Information Security Governance framework, as discussed in the next section. Each component addressed by a specific approach is indicated on Table 5 by an inclusion tick ("•"). The sum of the ticks is divided by the total number of components to give the percentage of representation for each approach. This is depicted at the bottom of the table (ISO17799—68%, Eloff and Eloff—63%, McCarthy and Campbell—77%, and Tudor—59%).

Based on the assessment of the approaches, the components of ISO/IEC 17799 (2005) and the Capability Maturity Model of McCarthy and Campbell are the most comprehensive in addressing the breadth of information security components and therefore the percentage representation is higher compared to the approach of Eloff and Eloff and Tudor. Corporate governance, ethical conduct, and trust are not included in either of these two approaches, although all three components are considered by various researchers (Donaldson, 2005; Flowerday & Von Solms, 2006; Trompeter & Eloff, 2001) when governing information security in an organization.

The approach put forward by Eloff and Eloff (2005) suggests a holistic set of controls to consider and focuses mainly on providing a standardised approach for the management of an information security program. It is the only approach that mentions ethical values. Employees need to integrate

TABLE 5 Information Security Governance App

	Information security components	ISO 17799 (2005)	Eloff & Eloff	McCarthy & Campbell	Tudor
1	Corporate governance	X	X	X	X
2	Information security strategy	X	X	•	X
3	Leadership in terms of guidance and executive level representation	•	•	•	•
4	Security organization (internal organization such as management commitment, responsibilities, and coordination; external parties)	•	•	•	•
5	Security policies, standards, and guidelines	•	•	•	•
6	Measurement / Metric / Return on investment	X	•	•	X
7	Compliance and monitoring (legal, regulatory, and auditing)	•	•	•	•
8	User management (user, joiner, and leaver process)	•	X	•	X
9	User awareness, training, and education	•	•	•	•
10	Ethical values and conduct	X	•	X	X
11	Privacy	X	X	•	X
12	Trust	X	X	X	•
13	Certification against a standard	•	•	X	X
14	Best practice and baseline consideration	•	•	•	•
15	Asset management (responsibility and classification)	•	•	X	•
16	Physical and environmental controls (secure areas and equipment)	•	•	•	•
17	Technical operations (e.g., anti-virus, capacity, change management, and system development)	•	•	•	•
18	System acquisition, development, and maintenance	•	•	•	X
19	Incident management	•	X	•	X
20	Business continuity planning (BCP)	•	X	•	•
21	Disaster recovery planning (DRP)	X	X	•	•
22	Risk assessment process	•	•	•	•
Number of components derived from each approach		**15**	**14**	**17**	**13**
Percentage		**68%**	**63%**	**77%**	**59%**

ethical conduct or behavior relating to information security into their everyday life in the organization (Trompeter & Eloff, 2001). According to Baggett (2003), it is the responsibility of management and the board to develop and distribute corporate codes of conduct that should cover both commercial and social responsibilities. Ethical conduct, for example, not copying organizational software at home or using the Internet for private purposes during working hours, needs to be enforced as the accepted way of conduct in the work environment in order for the desired information security culture to emerge. Although the Eloff approach (Eloff & Eloff, 2005) is very comprehensive, it does not mention aspects such as business continuity or incident management. These could, however, be covered under the policy and procedures component.

Only Tudor (2000) mentions trust in his approach. According to Von Solms (2000), trust is arguably the most important issue in establishing information security in an IT environment. If management trusts its employees and the employees trust management, it is easier to implement new procedures and guide employees through changes of behaviour pertaining to information security. Corporate governance, ethical considerations and trust would all need to be incorporated into the approach adopted by an organization to provide a comprehensive set of information security components that can deal with its risks such as attempts at social engineering, fraud and staff misuse of information systems.

A NEW APPROACH TO AN INFORMATION SECURITY GOVERNANCE FRAMEWORK

In consolidating the four approaches towards information security governance discussed above,

one assembles a comprehensive set of c onsists of a comprehensive list of information security components categorised under each of the six main categories (level B). All six of the main categories are influenced by change depicted at the bottom of the figure (level D).

to consider for information security governance. The proposed Information Security Governance framework (see Figure 2) can be used as a starting point by an organization to govern information security by developing guidelines and implementing controls to address risks identified by the organizations, such as misuse of web browsing, data corruption, or identify theft. This new framework can be utilized to govern employee behavior in all required facets of information security and cultivating an acceptable level of information security culture.

Ultimately, this governance framework provides management the means to implement an effective and comprehensive information security governance program that addresses technical, procedural, and human components. It integrates the components of the four discussed approaches, as well as components not considered, such as trust. Hence, the framework provides a single point of reference for the governance of information security to inculcate an acceptable level of information security culture. As each organization's environment is different and subject to different national and international legislation and regulations, additional components might be required, while others may not be relevant.

The information security governance framework, Figure 2, is partitioned into four levels, namely A, B, C, and D. Level A consists of strategic, managerial/implementation and technical protection components. The strategic components, shown on the left side of the figure, provide direction to the managerial and operational implementation components, depicted in the middle section of the figure. The technical protection components are shown on the right side of Figure 2.

Level B consists out of six main categories which are grouped according to the three Level A categories. The six main categories are:

- Strategic:
  - Leadership and governance.
- Managerial and Operational:
  - Security management and organization;
  - Security policies;
  - Security program management; and
  - User security management.
- Technical:
  - Technology protection and operations.

Implementing the information security components institutes change in the organization's processes and will influence the way people conduct their work. An important consideration is that organizations do not change, but people do, and therefore people change organizations (Verton, 2000). Information security changes in the organization need to be accepted and managed in such a way that employees are able to successfully incorporate such changes into their work. The component indicated as "Change" (Figure 2), needs to be considered when implementing any of the information security components. The six main categories (level B) of information security components and the composition thereof are discussed below.

Leadership and Governance

This category comprises executive level sponsorship for information security, as well as commitment from the board and management to protect information assets. This is due to the fact that information security governance is accepted as an integral part of good IT and Corporate Governance (Von Solms, 2005). Corporate governance refers to organization controls such as reporting structure, authority, ownership, oversight, and policy enforcement (Knapp, Marshall, Rainer, & Morrow, 2004). Corporate governance relates to the responsibility of the board to effectively direct and control an organization through sound leadership efforts (King Report, 2001; Donaldson, 2005). This is associated with IT governance, which is concerned about the policies and procedures that define how an organization will direct and control the use of its technology and protect its information (Posthumus & Von Solms, 2005).

Based on a study conducted by Gartner (Security, 2005), some of the top 10 business and technology priorities of Chief Information Officers (CIOs) in 2005 were to implement security enhancement tools, and to address security breaches and disruptions, as well as privacy issues. These actions would illustrate that

management is realising that information can add great value to the organization – which is the starting point for illustrating information security leadership.

The leadership and governance category also involves the compilation of an information security strategy that addresses information threats by conducting risk assessments aimed at identifying mitigation strategies and required controls. The information security strategy should be linked to the organizational and IT strategy to ensure that the organization's objectives are met both in the short and in the long term.

Finally, the category includes the concepts of metrics and measurement to measure how effective the organization is in addressing threats to information security. Many organizations are turning to metrics to evaluate the overall effectiveness of their information security programs (Witty & Hallawell, 2003) and whether it contributes in achieving the organization's strategy. The number of security incidents or even empirical results of awareness surveys can be used as metrics. Metrics will assist organizations in converting today's security threats into tomorrow's business opportunities (Ponemon, 2005).

Security Management and Organization

Program organization and legal and regulatory considerations are covered in this category. The objective of the category is to manage information security within the organization (ISO 17799, 2005). Program organization refers to the information security organizational design, composition and reporting structures (e.g., centralized or decentralized management of security). It also incorporates the roles and responsibilities, skills and experience, and resource levels committed to the enterprise security architecture (McCarthy & Campbell, 2001).

Different pieces of national and international legislation need to be considered for information security—for example, the Health Insurance Portability and Accountability Act (HIPAA) (Bresz, 2004); the Sarbanes-Oxley Act (Donaldson, 2005); the King Report II (2001); the Electronic Communications and Transactions Act (ECT) (2002); and the Promotion of Access to Information Act (PROATIA) (2000).

Security Policies

Security policies, procedures, standards, and guidelines are key to the implementation of information security in order to provide management with direction and support (ISO 17799, 2005) and they should clearly state what is expected of employees and guidelines for their behavior (Richards, 2002). ISO 17799 (2005) defines a policy as an "overall intention and direction as formally expressed by management." The security policies should consider the categories mentioned earlier (e.g., legal considerations) and must be implemented in the organization through effective processes and compliance monitoring. Examples of information security policies are an access control policy, e-mail, and Internet policy and a physical and environmental policy. A procedure such as a user registration and deregistration procedure explains or spells out statements of the security policy and is the steps that need to be taken to accomplish the policy (Von Solms & Von Solms, 2004). Procedures are underpinned by standards such as a password standard and guidelines for example how to configure a firewall to meet the requirements of the security policy.

Security Program Management

Monitoring and compliance as well as auditing are included in this category, which involves management of the security program. It is essential to measure and enforce compliance (Von Solms, 2005), and both technology and employee behavior (Vroom & Von Solms, 2004) should be monitored to ensure compliance with information security policies and to respond effectively and timely to incidents that are detected. Monitoring of employee behavior could include monitoring the installation of unauthorized software, the use of strong passwords or Internet sites visited. Technology monitoring could relate to capacity and network traffic monitoring. Information security auditing is necessary to ensure that the policies, processes, procedures and controls are in line with the objectives, goals and vision of the organization (Vroom & Von Solms, 2004).

User Security Management

This category addresses user awareness; education and training; ethical conduct; trust and privacy. ISO/IEC 17799 (2005) states that the organization must have plans and programs in place to implement, maintain, and effectively promote information security awareness and education throughout the organization.

According to the Guidelines for the Security of Information Systems and Networks of the Organization for Economic Cooperation and Development (OECD) (Baggett, 2003), one of the principles in creating a security culture is ethical conduct—where both management and the board develop and communicate corporate codes of conduct. Hellriegel, Slocum, and Woodman (1998) define ethics as the values and rules that distinguish right from wrong. It is management's responsibility to establish ethical standards of conduct that are in essence rules to be followed by employees and to be enforced by the organization (Cardinali, 1995). As part of the information security governance framework, ethical conduct must be addressed by the organization to minimize the risk of for instance invasion of privacy, selling of customer information and unauthorised altering of data. These rules should be communicated to employees as part of the security awareness programme.

N. Martins (2002) defines trust as "the process in which a trustor relies on a trustee (a person or group of people) to act according to specific expectations that are important to the trustor without taking advantage of the trustor's vulnerability." When implementing the Information Security Governance framework components, management must be able to trust employees to adhere to information security policies, while employees must be able to trust management to demonstrate commitment to information security (trust is seen as the primary attribute of leadership) (Robbins, Odendaal, & Roodt, 2001). A trusting relationship should also be established between trading partners and clients who could contribute to the organization's reputation. One possible way of establishing such a relationship could be for the organization to illustrate that information and assets are secured and that employees comply with requirements.

; an essential issue of trust when it comes to good relationships with customers, suppliers and other business partners (Tretic, 2001). If there is no privacy in business, there will be no trust (Ross, 2000). When implementing information security privacy, both employees and customers must be considered and controls must be implemented to protect their identity.

Technology Protection and Operations

The technology protection and operations category relates to the traditional focus of information security. It involves the technical and physical mechanisms implemented to secure an IT environment (Von Solms, 1997; Von Solms, 2000). When implementing the security governance framework, the technology controls applicable to the organization's environment and identified risks must be implemented. These include asset management, system development requirements, incident management, technical operations such as network security, and physical, environment, and business continuity controls. It is essential that the technology environment be monitored on a constant basis and that the risks of technology changes in the market be addressed—e.g., the use of personal digital assistants and teleworking technology.

CONCLUSION

The first step in developing an information security culture and empowering the workforce to be aware of their responsibilities towards protecting information assets would be to implement a comprehensive Information Security Governance framework—as is proposed in this article. It is evident that one approach alone is not sufficient in governing information security, but that an integrated approach should be adopted to ensure that all components pertaining to information security is considered. The new Information Security Governance framework can be deployed by organizations as a comprehensive and single point of reference towards governing information security. It considers a broad spectrum of components to assist in addressing risks to infor-

mation assets on a technology, processes level. Management and executives can use the Information Security Governance framework as a reference for governing information security in all facets of the organization's information asset environment. The implementation of the applicable components of the Information Security Governance framework in an organization should have a positive impact on the behavior of employees and on how they protect the organization's assets, thereby minimising risks to information assets and cultivating an acceptable information security culture. The governance framework can be used in future research as a reference to develop an information security culture assessment tool to measure whether the level of information security culture is on an acceptable level, and to employ action plans for areas of development.

References

Baggett, W. O. (2003). Creating a culture of security. *The Internal Auditor*, *60* (3), 37–41.

Bresz, F.P. (2004). People—Often the weakest link in security, but one of the best places to start. *Journal of Health Care Compliance*, *6* (4), 57–60.

Cardinali, R. (1995). Reinforcing our moral vision: Examining the relationship between unethical behaviour and computer crime. *Work Study. 44* (8), 11–18.

COBIT security baseline—An information security survival kit. (2004). Rolling Meadows, USA: IT Governance Institute.

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

Donaldson, W. H. (2005). U.S. capital markets in the post-Sarbanes-Oxley world: Why our markets should matter to foreign issuers. *U.S. Securities and Exchange Commission*. London School of Economics and Political Science.

Electronic Communications and Transactions Act. (2002). Retrieved 12 January 2006 from site: http://www.acts.co.za/ect_act/

Eloff, J. H. P. & Eloff, M. (2005). Integrated Information Security Architecture, *Computer Fraud and Security*, *2005* (11), 10–16.

Flowerday, S., & Von Solms, R. (2006). Trust an element of information security. In *Security and Privacy in Dynamic Environments*. IFIP/SEC2005; Boston: Kluwer Academic Publishers, 87–97.

Hellriegel, D., Slocum, J. W. (Jr), & Woodman, R. W. (1998). *Organizational Behavior*. (8th ed.). Cincinnati, OH: South-Western College Publishing. Holborn Books. Information Security architecture: An integrated approach to security in the organization (2005). Retrieved 18 April 2005 from: http://www.holbornbooks.co.uk/details.aspx?sn=1244811

ISO/IEC 17799 (BS 7799-1) (2005). Information technology. Security techniques. Code of practice for information security management, Britain.

ISO/IEC 27001 (BS 7799-2) (2005). Information technology. Security techniques. Information security management systems—requirements, Britain.

King Report. (2001). The King Report of corporate governance for South Africa. Retrieved 12 January 2006: http://www.iodsa.co.za/downloads/King%20II%20Report%20CDRom%20Brochure.pdf

arshall, T. E., Rainer, R. K., & Morrow, D. W. (2004). Top ranked information security issues: *The 2004 International Information Systems Security Certification Consortium (SIC) survey results*. Auburn, Alabama: College of Business Auburn University.

McCarthy, M. P. & Campbell, S. (2001). *Security Transformation*. McGraw-Hill: New York.

Martins, A. (2002). *Information Security Culture*. Master's dissertation, Rand Afrikaans University, Johannesburg, South Africa.

Martins, A. & Eloff, J. H. P. (2002). Information Security Culture. In *Security in the information society. IFIP/SEC2002*. (pp. 203–214). Boston: Kluwer Academic Publishers.

Martins, N. (2002). A model for managing trust. *International Journal of Manpower. 23* (8), 754–769.

The Concise Oxford Dictionary. (1983). Sykes, J.B. (Ed.) Oxford: Clarendon Press.

Posthumus, S. & Von Solms, R. (2005). IT Governance. *Computer Fraud and Security. 2005* (6), 11–17.

PriceWaterhouseCoopers. Information Security Breaches Survey. (2004). Retrieved 12 March 2005 from http://www.dti.gov.uk/industry_files/pdf/isbs_2004v3.pdf

Promotion of Access to Information Act. (2000). Retrieved 12 January 2006 from http://www.acts.co.za/prom_of_access_to_info/index.htm

Richards, N. (2002). The critical importance of information security to financial institutions. *Business Credit*, *104* (9), 35–36.

Robbins, S. (2001). *Organizational Behaviour*. (9th ed.). New Jersey: Prentice Hall.

Ross, B. (2000). New directives beef up trust in e-commerce. *Computer Weekly News*.

Security. 2005. Security, innovation head CIO's 2005 agenda. *Computer Fraud and Security*, *2005* (1), 1–2.

Teufel, S. (2003). Information Security Management—State of the art and future trends. In *Proceedings of the Annual International Information Security South Africa (ISSA) conference*. Johannesburg, SA, UNISA Press.

Tretic, B. (2001 January). Can you keep a secret? *Intelligent Enterprise*. *4* (1).

Trompeter, C. M. & Eloff, J. H. P. (2001). A framework for the implementation of Socio-ethical controls in Information Security. *Computers and Security*, *20* (5), 384–391.

Tudor, J. K. (2000). *Information Security Architecture—An integrated approach to security in an organization*. Boca Raton, FL: Auerbach.

Verton, D. (2000). Companies aim to build security awareness. *Computerworld*, *34* (48), 24.

Von Solms, R. (1997). Driving safely on the information superhighway. *Information Management & Computer Security*, *5* (1), 20–22.

Von Solms, B. (2000). Information security—The third wave? *Computers and Security*, 19(7). November, 615-620.

Von Solms, S. H. (2005). Information Security Governance—Compliance management vs. operational Management. *Computers and Security*, *24* (6), 443–447.

Von Solms, S. H. (2006). Information Security—The fourth wave. *Computers and Security. 25* (2006), 165–168.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers and Security*, *23* (33), 191–198.

Witty, R. J. & Hallawell, A. (2003). Client issues for security policies and architecture. *Gartner*. ID number: K-20-7780.

BIOGRAPHIES

Adele da Veiga is currently completing her PhD (IT) focusing on information security culture at the University of Pretoria, South Africa. She is a management consultant focusing on information security, risk management, and auditing.

JHP Eloff received a PhD (Computer Sc[illegible]f Pretoria. He has published extensively the Rand Afrikaans University, South Africa. He gained practical experience by working as management consultant specializing in the field of information security. He is the Head of Department and full professor in Computer Science at the Department of Computer Science, in a wide spectrum of accredited international subject journals. He is evaluated as a B2 researcher from The National Research Foundation (NRF), South Africa. He is a member of the Council for Natural Scientists of South Africa.