# CORPORATE INFORMATION SECURITY EDUCATION:

*Is Outcomes Based Education the Solution?*

Johan Van Niekerk [1] And Rossouw Von Solms [2]

*Department of Business Information Systems, Port Elizabeth Technikon[1]; Department of Information Technology, Port Elizabeth Technikon[2]*

**Abstract:** Today's global economy is increasingly dependent on the creation, management, and distribution of information resources. Information and its use permeate all aspects of modern society. Most modern organizations need information systems to survive and prosper. Information has become a valuable commodity and as such needs to be protected. This protection is typically implemented in the form of various security controls. In order for these controls to be effective, the users in the organization need to be educated regarding these controls. Recent studies have indicated that current user education programs fail to pay adequate attention to behavioral theories. This paper examines the educational principles an information security user education program should adhere to. It then introduces outcomes based education (OBE) and finally argues that OBE is ideally suited for the needs of information security.

**Key words:** Information Security, Information Security Culture, Outcomes Based Education, Awareness

## 1. INTRODUCTION

In today's business world, information is a valuable commodity and as such, needs to be protected. Information affects all aspects of today's businesses, from top management right down to the operational level (Turban, et al., 2002. pp 3-37). In order to avoid loss or damage to this valuable resource, companies need to be serious about protecting their information. This protection is typically implemented in the form of various security controls (Barnard & Von Solms, 2000). However, it is very difficult

to know exactly which controls would be required in order to guarantee an acceptable minimum level of security. Furthermore, managing these controls to see that they are always up to date and implemented uniformly throughout the organization is a constant headache to organizations.

When selecting the controls to implement in an organization, it is important to refer to accepted international standards (Von Solms, 1999). There exist several internationally accepted standards and codes of practice to assist organizations in the implementation and management of an organizational information security strategy. Some of the better known examples would include the ISO/IEC 17799 (British Standards Institute (BSI), 1999) and ISO/IEC 13335 also known as GMITS (Guidelines to the Management of Information Technology Security (GMITS), 1995).

These standards and codes of practice provide organizations with guidelines specifying how the problem of managing information security should be approached (Von Solms, 1999). One of the primary controls identified by many of the major IT security standards published to date is the introduction of a corporate information security awareness program (BSI, 1999; GMITS, 1995). The purpose of such a program is to educate the users about information security or, more specifically, to educate users about the individual roles they should play in the effective execution and maintenance of these controls. Most security controls, whether physical, technical, managerial or administrative in nature, requires some form of human involvement. This paper will examine this dependence of information security on human involvement with specific emphasis on the role user education has to play in a corporate information security strategy. It will then propose outcomes based education (OBE) as a pedagogical methodology suitable for the information security education needs of organizations.

## 2. THE HUMAN SIDE OF INFORMATION SECURITY

Information security controls can generally be sub-divided into three categories: Physical controls, Technical controls and Operational controls (Thomson, 1998, p. 29). Physical controls deal with the physical aspects of security, for example; the lock on the door of an office containing sensitive documents. Technical controls are controls of a technical nature, usually software based, for example; forcing a user to authenticate with a unique username and password before allowing the user to access the operating system. The third category, operational controls, collectively including

business-, administrative-, managerial-, and procedural controls, consist of all controls that deal with human behavior in one form or another. These controls would include those that deal with the creation of information security policies and procedures, and administration of other controls. Both physical and technical controls, even though they do not deal directly with operational issues, usually require some form of human involvement. In an organizational context, these controls would thus have to be supported by procedures outlining the employee's involvement in the use of these controls.

Employees, whether intentionally or through negligence, often due to a lack of knowledge, are the greatest threat to information security (Thomson, 1998, p. 12, Mitnick & Simon, 2002, p. 3). Operational controls rely on human behavior. This means that these controls are arguably some of the weakest links in information security. Unfortunately, both physical and technical controls rely to some extent on these operational controls for effectiveness. As an example, an operational control might state that a user leaving his/her office must logoff from the operating system and lock his/her office door. If a user were to ignore this procedure, both the technical control forcing authentication and the physical control of having a lock on the door would be rendered useless. Thus, anyone who thinks that security products, i.e. technical and physical controls, alone, offer true security is settling for the illusion of security (Mitnick & Simon, 2002, p. 4).

Siponen (2001) describes this tendency of organizations to settle for the illusion of security as a general human tendency to often blindly ignore complications in IT related issues. Without an adequate level of user co-operation and knowledge, many security techniques are liable to be misused or misinterpreted by users. This may result in even an adequate security measure becoming inadequate (Siponen, 2001) Organizations **cannot** protect the integrity, confidentiality, and availability of information in today's highly networked systems environment without ensuring that each person involved understands his/her roles and responsibilities and is adequately trained to perform them (National Institute of Standards and Technology (NIST), 1998, p. 3).

Teaching employees their roles and responsibilities relating to information security requires the investment of company resources in a user education program. However, budgetary requirements for security education and training are generally not a top priority for organizations (Nosworthy, 2000). Organizations often spend most their information security budget on technical controls and fail to realize that a successful information security

management program requires a balance of technical and business controls (Nosworthy, 2000). Business controls in this sense refer to operational controls. According to Dhillon (1999), increasing awareness of security issues is the most cost-effective control that an organization can implement. However, in order to ensure that the maximum return on investment is gained, special care should be taken to ensure the success of the user education programs used. For **educational** programs this would mean ensuring adherence to proper pedagogical principles when these educational programs are compiled.

Most current user education programs fail to pay adequate attention to behavioral theories (Siponen, 2001). The emphasis of user education programs should be to build an organizational sub-culture of security awareness, by instilling the aspects of information security in every employee as a natural way of performing his or her daily job (Von Solms, 2000). Recent studies have indicated that the establishment of an information security "culture" in the organization is desirable for effective information security (Von Solms, 2000). Such a culture should support all business activities in such a way that information security becomes a natural aspect in the daily activities of every employee (Schlienger & Teufel, 2003). A detailed examination of how such a culture could be established in an organization falls outside the scope of this paper. Instead this paper will focus only on user education, one of the cornerstones required for the establishment of such a culture. For more information on the establishment of such a culture see e.g. (Van Niekerk & Von Solms, 2003; Schlienger & Teufel, 2003).

## 3. ELEMENTS OF INFORMATION SECURITY EDUCATION

The user education programs needed for information security purposes differ from traditional educational programs. Unlike traditional educational programs, these programs will primarily be aimed at teaching adults. Adults have well established, not formative, values, beliefs, and opinions (NIST, 1998, p. 20). The educational methodology used should thus be suitable for adult education. Furthermore, there are several other requirements specific to the role that such a program will play in the overall organization's information security efforts. In the following sections, this paper will suggest and attempt to motivate some of the features that should typically constitute such an information security education program.

## 3.1 Everyone should be able to "pass" the course.

Nosworthy (2000) states that each person in the organization from the CEO to House Keeping staff must be aware of, and trained to exercise their responsibilities towards information security. However in traditional educational models there are usually a percentage of the learners who do not pass the course, or in other words, successfully meet the assessment criteria. In order for an organization's information to be secure, everyone needs to not only be trained, but to "pass" the training. Unlike traditional education, failing an information security educational program cannot be accepted. Workers at every level, even those who do not use a computer, are liable to be targeted (Mitnick & Simon, 2002, p. 39). This means that having even a single person who does not know his/her information security responsibilities should be unacceptable.

## 3.2 Employees must know why information security is important and why a specific policy or control is in place.

Recent studies have suggested that current information security awareness programs are failing (Siponen, 2001). This failure is due to many reasons. Schlienger & Teufel (2003) have shown that even employees who know their responsibilities with regards to information security will still disobey security policy if they disagree with the policy. They suggest that the mere awareness of the policies and procedures is in fact not sufficient, the users also need to know why a specific policy or control is in place (Schlienger & Teufel, 2003). In information security, being taught why a specific policy or control is in place is generally considered to be a feature of education, and not of awareness (Schlienger & Teufel, 2003; NIST, 1998, pp. 16-17). Information security "education" is generally sub-divided into three levels, namely; awareness, training and education. Awareness simply focuses attention on information security. Training is more interactive and tries to instill the necessary skills and competencies. Education integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge and adds a multi-disciplinary study of concepts, issues, and principles (NIST, 1998, pp. 15-16). A feature of the educational level is that the user must understand why information security is important (Schlienger & Teufel, 2003; NIST, 1998, pp. 16-17). Obviously end-users do not require the same level of understanding as information security professionals (NIST, 1998, p. 14). You don't need to understand why procedures are in place or how the technologies work to use them

effectively (Tripathy, 2000; NIST 1998, p. 15). However, in information security, if a user asks why, it should always be explained (Tripathy, 2000).

## 3.3 Learning materials should be customized to the needs of individual learners.

In an organizational context, users of information exist at several levels. There are essentially three categories of users that need to be educated in information security awareness namely: The End User, IT Personnel and Top Management (Thompson, 1998). The National Institute for Science and Technology (NIST) expands on this classification by stating that training and education are to be provided selectively, based on individual responsibilities and needs. Specifically, training is to be provided to individuals based on their particular job functions (NIST, 1998, p. 43). The ISO/IEC 17799 states that the information security policy should be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader (BSI, 1999, p. 3). According to NIST, individuals learn in several ways, but each person, as part of his/her personality, has a preferred or primary learning style. Instruction can positively, or negatively, affect a student's performance, depending on whether it is matched, or mismatched, with a student's preferred learning style (NIST, 1998, p. 19). Thus, what should be taught to a specific individual user and how it should be taught, will depend on both the user's preferred learning style, and the specific role that user plays within the organization.

## 3.4 Users should be responsible for their own learning.

In today's organizations it is crucial to maximize return on investment. Through its very nature classroom training requires the availability of highly trained specialists to present the courses. It also requires that the learners take time off from their regular duties to attend classes. These factors make classroom training very expensive. One of the most cost-effective substitutes for traditional classroom training is to provide employees with intranet-based instruction (O'Brien, 1999, p.361). Such web-based instructional programs require individual learners to be responsible for their own acquisition of knowledge instead of being passive receptors in the process (ITiCSE Working Group on the Web and Distance Learning, 1997). Self-driven learning also enables organizations to make learning material available in a variety of formats. This is turn means users will have a choice of how they

are taught, which has already been shown to be a necessary feature of information security education.

## 3.5 Users should be held accountable for their studies.

Most information security standards make it clear that users should be held accountable for their information security **responsibilities** (BSI, 1999, pp. 8-10). These responsibilities are normally spelt out in the organization's information security policies and procedures. In an organization, policies function in a similar fashion to laws. For laws, ignorance is not a valid defense. However ignorance of policy is an acceptable defense (Whitman & Mattord, 2003, p. 93). Thus, to be able to hold employees accountable for their **actions,** the organization should have proof, normally in the form of a signed form, that the employees have been educated regarding their responsibilities and that they understand and accept these responsibilities as laid out in the policies (Whitman & Mattord, 2003, p. 93). Wood (1997) suggests that all employees should be required, on an annual basis, to sign a statement saying that they have read and understood the information security policy manual. It should thus be clear that self-driven learning for information security purposes, as discussed previously, could only be used if the employees are also held accountable for their learning. Otherwise the organization could not legally hold the employees accountable for their actions.

Many organizations have realized that their own employees are the biggest threat to their information systems (Von Solms, 2000). However, through the establishment of a culture of information security, users can become a security asset instead of being a threat (Von Solms, 2000). Education of employees plays a very important role in the establishment of such a culture. It is paramount that the people are educated to want to be more secure in their day to day operation (Nosworthy, 2000). Such a change of attitude is of utmost importance, because a change in attitude automatically leads to a subsequent behavioral change (Nosworthy, 2000). The employees can then become the organization's most valuable assets. Current programs used to educate employees, fails to pay sufficient attention to aspects related to the behavioral sciences (Siponen, 2001).

It would make sense to adhere to a formal educational methodology when constructing such educational programs. The methodology used should be suitable for the specific needs of an information security user education program. Since the aim of the user education program is not to prepare the users for further levels of formal education, but rather to help them achieve

information security know-how for use in their everyday jobs, the educational methodology used should be chosen accordingly. Outcomes Based Education (OBE) is an educational methodology that might in fact be ideally suited for use in such programs. The aim of OBE is to help learners achieve a specific outcome, in this case information security awareness and know-how.

## 4. OUTCOMES BASED EDUCATION

OBE is defined as an approach to teaching and learning which stresses the need to be clear about what learners are expected to achieve. The educator states beforehand what "outcome" is expected of the learners. The role of the educator is then to help the learners achieve that outcome (Siebörger, 1998).

Outcomes can be defined as either cross-curriculum (general outcomes) or specific outcomes. A cross-curriculum outcome can be seen as the desired effect that attaining a specific competency should have within the general environment within which the learner operates. A specific outcome is one that directly demonstrates the mastery of the appropriate skill that the learner should gain from the OBE program.

For each outcome an assessment standard should be defined. These standards are necessary in order to provide feedback to the learners. According to Siebörger (1998) assessment is essential to OBE to measure the degree to which a learner has achieved an outcome. In fact being able to assess progress and provide feedback to the learner is a prerequisite for any educational program to be successful. Fingar (1996) states that feedback, specifically in the form of knowledge regarding the outcomes of the learners' actions, is required for learning to take place. Furthermore this feedback should be continuous and constructive (Department Of Education (DOE), 2001).

The educational process in general can be viewed as a system of teaching and learning activities that are tied together via various feedback loops. It also includes other functions such as assessment, admission, quality assurance, direction and support (Tait, 1997). All of these components can, and should, play a role in the creation of an effective information security education program. OBE can be viewed in three different ways: as a theory of education, a systematic structure for education, or the creation of educational material, and lastly as a classroom practice (Killen, 2000). OBE

can thus be seen as a complete educational system, which contains all the components such a system should have.

According to Killen (2000), OBE is based upon three basic premises, namely:

1. All students can learn and succeed, but not all in the same time or in the same way.
2. Successful learning promotes even more successful learning.
3. Schools (and teachers) control the conditions that determine whether or not students are successful at learning.

From these basic premises four essential principles of OBE were developed (Killen, 2000). They are:

1. Clarity of focus, which means that all teaching activities must be clearly focused on the desired outcome that the learners should achieve.
2. Designing back, which means that the starting point for an OBE program's design should be a clear definition of the desired results. The rest of the curriculum should be designed according to this desired outcome.
3. High expectations for all students. OBE not only assumes that everyone can attain the desired outcomes, it also requires that high standards should be set. This is based on evidence that learners are more likely to attain high standards when they are challenged by what is expected from them.
4. Expanded opportunities for all learners. This final principle of OBE is based on the idea that not everyone learns the same way or at the same pace. Thus, in OBE, learners are given many opportunities for learning. Achieving the desired outcome is deemed more important than how that outcome was reached.

In order for an educational program to be classified as being outcomes based, it has to adhere to all four of these principles.

## 5. OUTCOMES BASED EDUCATION FOR INFORMATION SECURITY

Up to this point this paper has shown the requirements an educational methodology would have to meet in order for it to be suitable for information security education. It has also introduced OBE and briefly outlined the basic premises and the principles of this educational

methodology. It will now attempt to show that OBE is in fact well suited to the needs of information security.

The first requirement listed for information security education was that everyone should be able to "pass" the course. Clearly OBE fulfils this requirement since the first premise upon which OBE is based is the assumption that all students can succeed and learn.

Secondly, for information security education to be successful, employees must know why information security is important and why a specific policy or control is in place. Course developers should be aware that adults have well-established values, beliefs, and opinions. Adults relate new information and knowledge to previously learned information, experiences, and values which might result in misunderstanding (NIST, 1998, p. 20). It is even possible that they understand correctly but still don't adhere to a security policy because it conflicts with their beliefs and values (Schlienger & Teufel, 2003). One of the fundamental differences between OBE and traditional educational models is the fact that rote learning is completely unacceptable in OBE. OBE requires the learner to identify and solve problems in which responses display that responsible decisions using critical and creative thinking have been made (Olivier, 1998; Pretorius, 1998). This type of thinking requires not only knowledge but also insight. Insight requires the learner to know why they are doing something (NIST, 1998, p. 18). According to Killen (2000) each outcome based educational program must have a rationale to explain why the program exists.

The third requirement of information security education identified was that learning materials should be customized to the needs of individual learners. The first basic premise of OBE not only states that all students can learn and succeed, but it also states that all students cannot necessarily do this in the same time or in the same way. This premise is also expanded on in the fourth principle of OBE, which states that learners should be given many opportunities for learning. OBE thus recognizes that individuals learn in different ways and at different paces. For a program to be truly outcomes based it is vital that learning materials are provided in as customized a format as possible for individual learners. However, according to Killen (2000) the practical difficulties of providing expanded opportunities must be weighed against the long-term benefits of enabling all learners to be successful.

The fourth and fifth suggested requirements of information security education state that users should be both responsible and accountable for

their own learning. In other words, the users should take ownership of their own learning. Ownership of their learning and self-driven learning are central concepts to OBE. Because OBE recognizes that different students will learn at a different pace, OBE encourages self-driven learning. The ability to effectively manage one's own time, and learning abilities, are one of the critical cross curriculum outcomes identified for all South African students (South African Qualification Authority (SAQA), 2000). The OBE model strives to move away from teacher centeredness, towards learner-centered education (Malan, 2000). Thus, responsibility for their own studies can be seen to be central to OBE. Hand in hand with responsibility is accountability. OBE places major emphasis on assessment as a tool to provide feedback on progress to the learner, and as a tool for measuring whether the desired outcomes have been reached (Killen, 2000; Malan, 2000). Assessment makes students accountable for their studies.

The following is a brief summary of the relationships between OBE and information security education concluded thus far:

1. In terms of an organization's overall information security effort it is vital for all users to ultimately pass the information security course. OBE requires a high expectation for all learners to do well, and additionally requires that learners be given multiple opportunities to prove that they have achieved the desired outcomes.
2. Employees should be told why a specific information security policy, or control, that applies to them, is in place. In OBE memorization of concepts is not sufficient, OBE requires learners to have insight and thus to understand why they are doing something.
3. Due to the different levels of prior education, different organizational roles and different individual preferences of employees in an organization, learning materials used in an organization should be customized to the needs of individual learners. Recognizing that individuals learn in different ways and at different paces are concepts central to OBE. Flexible learning material, to suit individual needs, is a pre-requisite in an outcomes based program.
4. In order to control costs, and to provide the above-mentioned flexibility in learning materials, organizational learners should be responsible for their own learning. The organization should supply the learning materials in formats that support as many learning styles as possible, but responsibility for using those materials should ultimately rest with the individual employees. Employees should thus take ownership of their learning. This concept of ownership and self-driven learning are central to OBE, which is essentially a learner centered educational methodology.

5. Hand-in-hand with ownership and responsibility is accountability. Organizations need to make employees accountable for their own learning, otherwise, they would not be able to hold them accountable for negligence stemming from a lack of education. In OBE, and other educational methodologies, assessment plays a vital role. Learners must be held accountable for their learning in order to get them to accept ownership of their learning.

OBE can thus be seen to match all of the requirements for information security education identified by this paper. In fact, a closer examination of the "results-based" educational framework advocated by NIST (1998) for information security programs will reveal many elements that are common to OBE as well. For example, NIST argues that information security education programs should be "results-based" and should focus on job functions, or roles and responsibilities specific to individuals (NIST, 1998, p. iii). OBE aims to help learners achieve a specific outcome or attain a specific skill. These outcomes should reflect the complexities of the real life and the roles the learners would have to fulfill (Killen, 2000). In an organizational context this would mean that the outcomes would have to reflect skills needed in the individual's day-to-day job functions. Several other such similarities exist, but a detailed examination of these falls outside the scope of this paper. Instead, the contextual role of OBE in the establishment of a corporate culture of information security will be briefly examined.

According to Van Niekerk and Von Solms (2003), establishing a corporate culture will have to start with top management, who has to show commitment to information security via vision statements, policies and their own behavior. Secondly, a user education program should be constructed to educate the users about these policies and the behavior expected from them. Thirdly, middle management will have to positively reinforce any learning that took place by giving continuous feedback to the users. This feedback could take the form of performance metrics, e.g. key performance indicators, for individual employees. Ultimately, it will be this continuous reinforcement by middle management that produces the change in behavior.

If OBE is to be used in this process, the cross-curriculum outcomes and measurables for these outcomes would have to be clearly defined. The programs to teach employees the necessary skills to attain these outcomes would then have to be drawn up and made available in a variety of learning formats. These could for example include a set of online tutorials, security manuals, videos or even lunch-hour workshops. This will ensure that each

user has a choice in terms of *how* they learn, which satisfies the third requirement as outlined previously. Part of these programs would have to discuss the possible consequences to both the individual and the organization as a whole, should an employee fail to comply to the taught procedures. This will satisfy the requirement that user should know why they are taught a skill.

Finally, to ensure that the users take ownership of their own learning, and to hold them accountable for their own learning, compliance metrics should be gathered. These metrics could then be used as part of individual user's key performance indicators. This can fulfill the role of the continuous feedback from middle management that is required to change behavior. These metrics could be gathered per department, branch, etc. and can then also be made part of the key performance indicators for the appropriate middle level manager. The old adage that what you measure is what you get will then play its part by ensuring that the appropriate line managers will feed this statistics back to their staff since it impacts on their own performance evaluations. Since the learning material should always be available and the employees are measured against their compliance, eventually all the users should reach a level of compliance that indicates they have "passed" the course. It should thus be very possible to integrate all the requirements of information security education, as identified in this paper, into the process aimed at introducing a change in the organizational culture, as outlined by Van Niekerk and Von Solms (2003).

## 6. CONCLUSION

Humans today live in an emerging global information society, with a global economy that is increasingly dependent on the creation, management, and distribution of information resources. Information and its use permeate all aspects of modern society. Today, most organizations need information systems to survive and prosper. It is therefore imperative that modern organizations, operating in this global information society, take the protection of their information resources seriously.

This paper has pointed out that this protection of information resources are to a large extent dependent on human co-operated behavior. It also pointed out that this dependence on human behavior makes it necessary to have a user education program to educate users regarding their roles and responsibilities towards information security. This paper proposed several "elements", or properties such an information security education program

should have in order for it to suit the needs of modern organizations. These included:

- Everyone should be able to "pass" the course.
- Employees must know why information security is important and why a specific policy or control is in place.
- Learning materials should be customized to the needs of individual learners.
- Users should be responsible for their own learning.
- Users should be held accountable for their studies.

Each of these proposed elements were argued in earlier sections of this paper.

The same elements were shown to be present in OBE, an existing pedagogical methodology. The possible role of OBE in the context of attempting to change organizational culture, were also briefly examined. This paper argued that OBE could be seen to be an excellent fit for the needs of information security education and is definitely **a** solution to these needs. It has been suggested that information security, because it depends on human behavior, should look at the human sciences when attempting to solve problems relating to the roles humans play in information security. This paper aims to reinforce that suggestion. Educationalists spend many years developing models such as outcomes based education (OBE). These models have been extensively tested and critically examined in the literature. It is the contention of this paper that instead of "re-inventing the wheel" when designing user education programs, information security practitioners should "borrow" methodologies, like OBE, from the educational sciences. Future researchers who wish to solve information security education problems should be basing their work on sound pedagogical models.

## REFERENCES

Barnard, L., Von Solms, R. (2000). A Formalized Approach to the Effective Selection and Evaluation of Information Security Controls. Computers and Security, 19(2): pp. 185-194.

British Standards Institute (BSI) (1999), BS 7799 Part 1: Code of Practice for Information Security Management (CoP), BSI, UK.

Dhillon, G. (1999) Managing and controlling computer misuse, Information Management *&* Computer Security, 7 (4), pp. 171-175.

Department of Education (DOE). (2001) Draft Revised National Curriculum Statement: Technology Learning Area. Department of Education. Available at:
http://education.pwv.gov.za/DoE_Sites/Curriculum/New_2005/draft_revised_national_curriculu.htm

Fingar, P. (1996). The blueprint for business objects. New York, New York : SIGS Books & Multimedia

Guidelines to the Management of Information Technology Security (GMITS). (1995). Part 1, ISO/IEC, JTC 1, SC27, WG 1.

ITiCSE Working Group on the Web and Distance Learning (1997). The Web and distance learning:what is appropriate and what is not. ITiCSE'97 Working Group Reports and Supplemental Proceedings, pp. 27-37.

Killen, R. (2000). Outcomes-Based education: Principles and Possibilities. Unpublished manuscript, University of Newcastle, Faculty of Education. [WWW document]. URL http://www.schools.nt.edu.au/curricbr/cf/outcomefocus/killen_paper.pdf. Sited 20 August 2003.

Laudon, K. C., Laudon, J. P. (2002). Management Information Systems: Managing the Digital Firm (7th ed). New Jersey, USA: Prentice Hall.

Malan, S.P.T. (2000) The 'new paradigm' of outcomes-based education in perspective. Tydskrif vir Gesinsekologie en Verbruikerswetenskappe (28), South Africa.

Martins, A., Eloff, J.H.P. (2002) Assessing Information Security Culture. ISSA 2002, Muldersdrift, South Africa, 10-12 July 2002.

Mitnick, K.D., Simon, W.L. (2002) The art of deception: Controlling the human element of security. United States of America: Wiley Publishing, Inc.

National Institute of Standards and Technology (NIST). (1998). Information Technology Security Training Requirements: A Role- and Performance-Based Model. NIST Special Publication 800-16. U.S. Government Printing Office, Washington.

Nosworthy, J. D. (2000) Implementing Information Security In the 21st Century – Do You Have the Balancing Factors? Computer & Security (19), pp. 337- 347. Elsevier Science Ltd.

O'Brien, J. A. (1999) Management Information Systems: Managing Information Technology in the Internetworked Enterprise (4th ed.). United States of America: Irwin/McGraw-Hill.

Olivier, C. (1998), Educate and Train : Outcomes-Based. Pretoria, South Africa. J.L. van Schaik.

Pretorius, F. (1998). Outcomes-based Education in South Africa. Randburg, South Africa: Hodder and Stoughton Educational.

South African Qualifications Authority (SAQA) (2000). The National Qualifications Framework and Curriculum Development. Retrieved on 10 September 2003 from URL http ://www. saqa.org.za

Schlienger, T., Teufel, S. (2003) Information Security Culture – From Analysis to Change. Proceedings of the 3rd Annual Information Security South Africa Conference, 9-11 July 2003, Sandton, South Africa, pp. 183-196.

Siebörger, R. (1998). Transforming Assessment: A guide for South African teachers. Cape Town, RSA: JUTA.

Siponen, M.T. (2001). Five Dimensions of Information Security Awareness. Computers and Society, June 2001. Pp. 24-29.

Tait, B. (1997). Object Orientation in educational software. Innovations in Education and Training International, 34 (3). Pp. 167-173.

Thomson, M. (1998). The development of an effective information security awareness program for use in an organization. Unpublished master's thesis. Port Elizabeth Technikon, Port Elizabeth, South Africa.

Tripathi, A. (2000) Education in Information Security. IEEE Concurrency, October-December 2000, pp. 4-8.

Turban, E., Mclean, E., Wetherbe, J. (2002). Information technology for management: Transforming business in the digital economy (3rd Ed).United States of America. John Wiley & Sons, inc.

Van Niekerk, J., Von Solms, R. (2003). Establishing an Information Security Culture in Organisations: An Outcomes Based Education Approach. Proceedings of the 3rd Annual Information Security South Africa Conference, 9-11 July 2003, Sandton, South Africa, pp. 3-12.

Von Solms, B. (2000) Information Security – The Third Wave? Computers & Security, 19 (7), pp. 615-620.

Von Solms, R. (1999) Information Security Management: why standards are important. Information Management & Computer Security, 7 (1), pp. 50-57.

Whitman, M. E., Mattord, H. J. (2003) Principles of Information Security. Canada: Thomson Course Technology.

Wood, C.C. (1997) Policies alone do not constitute a sufficient awareness effort. Computer Fraud & Security, December 1997, pp. 14-19.

## ACKNOWLEDGEMENTS

The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the author and are not necessarily to be attributed to the National Research Foundation.