ORGANISATIONAL LEARNING MODELS FOR INFORMATION SECURITY

Johan van Niekerk[a] and Rossouw von Solms[b]

[a]Department of Business Information Systems, Port Elizabeth Technikon
[b]Department of Information Technology, Port Elizabeth Technikon

[a]johanvn@petech.ac.za, 041 5043048, Private Bag X6011, PORT ELIZABETH, 6000
[b]rossouw@petech.ac.za, 041 5043604, Private Bag X6011, PORT ELIZABETH, 6000

ABSTRACT

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. The protection of information resources is to a large extent dependent on human co-operated behaviour. This dependence on human behaviour makes it necessary to have a user education program to educate users regarding their roles and responsibilities towards information security. Recent studies have indicated that current user education programs fail to pay adequate attention to behavioural theories. There exist several organisational learning models that could be used for information security education. This paper will examine some of these models in terms of their applicability to information security education.

KEY WORDS

Information Security, Information Security Culture, Outcomes Based Education, Awareness, Double-loop Learning, Organisational Learning

ORGANISATIONAL LEARNING MODELS FOR INFORMATION SECURITY

1 INTRODUCTION

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 (O'Brien, 1999, pp. 11). Information and its use permeate all aspects of modern society. Today, most organizations need information systems to survive and prosper (Laudon & Laudon, 2002, pp. 4). It is therefore imperative that modern organizations, operating in this global information society, take the protection of their information resources seriously.

This protection is typically implemented in the form of various security controls. Information security controls can generally be sub-divided into three categories: Physical controls, Technical controls and Operational controls (Thomson, 1998, p. 29; Van Niekerk & Von Solms, 2003). 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 (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). Such a culture would require employees to have knowledge of their information security responsibilities as well as commitment towards these responsibilities (Siponen, 2000). 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 components needed to establish such a culture. The rest of this paper will examine, and then briefly discuss, three learning models, which are arguably pedagogically sound, in an attempt to identify common principles an information security education program should adhere to if such a program is to be useful in the establishment of an organisational sub-culture of information security. In other words, this paper will try to examine pedagogically sound learning models. These models were selected based on the premise that information security involves standards, policies and user behaviour and that the selected models should be useable in an attempt to modify employee behaviour. The following three models will be examined:

- The American National Institute of Standards and Technology (NIST) model: "Information Technology Security Training Requirements: A Role- and Performance-Based Model" (Available online at http://www.nist.org as NIST special publication 800-16). This model is included because it is the American standard for information security training, and as such warrants closer examination.
- Organizational learning, including both single-, and double-loop learning. Organizational learning theories deal specifically with the idea of the organization as a whole learning and adapting its behaviour. These theories are widely used in the management sciences specifically to change employee behaviour, see e.g. (Rowe, 1996; Smith 2001:1; Smith 2001:2). Organizational learning theories are included in this study since they deal with both policies and employee behaviour.
- Outcomes based education (OBE). OBE is a pedagogical model used in schools in many countries world-wide. OBE is included in this paper due to the fact that it has been previously suggested as a driver for change in establishing an information security culture, see (Van Niekerk & Von Solms, 2003).

2 THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) MODEL

The American National Institute of Standards and Technology (NIST) provides an information security specific training model, see (NIST, 1998). This model provides a framework that serves as the American standard for information security training. The NIST model, entitled: "Information Technology Security Training Requirements: A Role- and Performance-Based Model", is currently the only standard that focus exclusively on learning as related to information security. The rest of this section will provide a brief overview of the NIST model.

The NIST model is based on the premise that learning is a continuum. Specifically, learning in this context starts with awareness, builds to training, and evolves into education (NIST, 1998, p.14). Furthermore the model is role-based. Meaning that it defines the IT security learning needed as a person assumes different roles within an organization and different responsibilities in relation to IT systems (NIST, 1998, p.14).

The premise that information security learning is a continuum consisting of awareness, training and education is fairly widely accepted see e.g. (Horrocks, 2001, Schlienger & Teufel, 2003). The three levels of learning in this continuum can be described as follows:

Awareness: The purpose of awareness programs is simply to focus attention on security issues. In awareness activities the learner is simply the recipient of information and do not actively participate (NIST 1998, p.15). Awareness campaigns often make use of tools such as posters, videos and promotional slogans.

Training: The learner has to know how he/she can behave securely. This level strives to produce relevant and needed security skills and competency by practitioners of functional specialties other than IT security (e.g., management, auditing). Training of special security tools or features within applications must be offered (NIST, 1998, p.16; Schlienger & Teufel, 2003).

Education: The "Education" level integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge. It also adds a multi-disciplinary study of concepts, issues, and principles (technological and social).This level strives to produce IT security specialists and professionals capable of vision and pro-active response (NIST, 1998, p.16). An important characteristic of education is that the employee must understand why information security is important for the organization (Schlienger & Teufel, 2003).

The model in NIST special publication 800-16 deals primarily with the training part of this learning continuum. The NIST document uses this continuum to identify the knowledge, skills, and abilities an individual needs to perform the IT security responsibilities specific to each of his or her roles in the organization. According to this model all employees would need awareness. Training would only be required by individuals whose roles in the company indicates a need for specific knowledge of security threats and risks, as well as the safeguards against these threats and risks. Lastly, according to this model, education would only be needed by information security specialists. Thus, the type of learning that individuals need starts simplistic and then becomes more comprehensive and detailed towards the top of the continuum. (NIST, 1998, pp. 13-14)

Once the specific information security related roles of an employee has been determined, the NIST document can be used to identify the specific learning requirements of that employee. The document also emphasizes that all learning materials should match individual learner preferences (NIST, 1998, p. 19). 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. Finally the document provides a framework for the planning of information security training curricula and the evaluation of training effectiveness. According to NIST special publication 800-16, evaluation of training is vital, and should be an integral component of any training programme (NIST, 1998, p. 157).

3 ORGANIZATIONAL LEARNING

According to Malhotra (1996) organizational learning could be defined as the process within organizations by which knowledge about action-outcome relationships and the effect of the environment on these relationships is developed. Most current organizational learning theories stem from theories originally developed by Chris Argyris and Donald Schon (Smith, 2001:1;Smith, 2001:2) These theories were based on the idea that people have mental maps with regard to how to act in situations. These maps involve the way people plan, implement and review their actions. Argyris and Schon asserted that it is these maps that guide people's actions, rather than the theories they explicitly espouse (Smith, 2001:2). Smith (2001:2) describes the process involved using a model based on three elements:

- Governing variables: Those dimensions that people are trying to keep within acceptable limits. In information security this could refer to acceptable levels of risk.
- Action strategies: The moves and plans people use to keep the governing variables within the acceptable range. In information security these would include procedures outlining employee behaviour in specific scenarios.
- Consequences: What happens as the result of an action. These would include both intended and unintended results.

Currently most organizations focus on adaptive, or single-loop, learning. Instead companies should be focussing on generative learning or "double-loop" learning (Malhotra, 1996, Rowe, 1996). Single-loop learning can be likened to a thermostat (Rowe 1996). If a thermostat learns it is too hot or too cold it will turn the heat on or off. It can do this because it receives information about the current temperature and it has the ability to take action through turning the heat on or off. Single-loop learning is usually present where the underlying governing variables, such as goals, values and frameworks, are taken for granted (Smith, 1996:2).

In order for organizational learning to take place, companies should be focussing on generative, or double-loop, learning (Malhotra, 1996). Generative learning emphasizes continuous experimentation and feedback in an ongoing examination of the very way in which organizations go about defining and solving problems. Thus it can be likened to a thermostat that has the ability to ask why it is set at a specific temperature and can then explore whether another setting might be more effective (Rowe, 1996). Double-loop learning could thus result in the underlying governing variables being adjusted should they be found to be ineffective or unrealistic. Fig 3.1 demonstrates the relationship between the three elements of the model and the two types of learning.

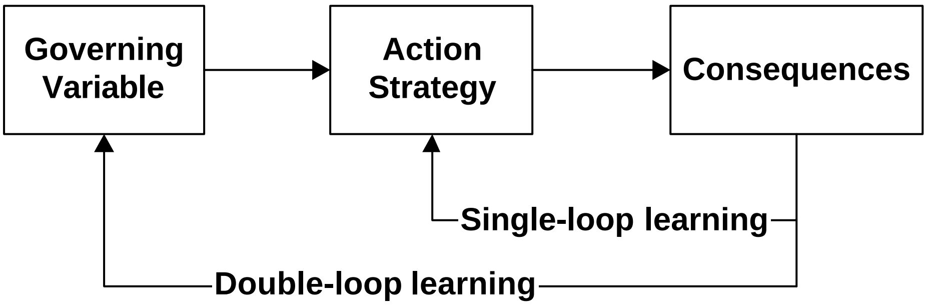

Figure 3.1: Organizational Learning (Adapted from Smith 2001:1)

4 OUTCOMES BASED EDUCATION (OBE)

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 (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 (Killen, 2000).
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 (Killen, 2000).

5 DISCUSSION

The previous sections provided a brief overview of three pedagogically sound models that could be applicable to corporate information security education. This paper will now attempt to identify, and briefly discuss, common characteristics and principles from these models.

Firstly, it should be clear that a proper learning program, even if it is aimed at corporate users, as opposed to students or scholars, requires a lot of planning. The NIST model provides extensive templates for planning training programs. OBE requires one to start with a clear view of the desired outcomes and then to design the curriculum based on the desired outcomes, taking into consideration the backgrounds and learning preferences of individuals. Organizational learning requires both the governing variables and desired action strategies to be taken into account when constructing learning programs. Efforts revolving around posters, videos or once-off classroom sessions can be said to fall within the awareness level of the continuum, which, though necessary, is not sufficient. It is therefore imperative for an organization to follow a formalized methodology, like e.g. the NIST templates and training matrixes, when constructing learning programs.

Secondly, in all three the models the outcome or the goal of the learning experience needs to be clearly defined. In the NIST model, templates for training programmes all start with clear goal statements, OBE has a clear statement of the desired outcomes as one of its core elements and organizational learning requires a definition of the desired consequences in order to evaluate the action strategies. In organizational learning, efforts focussing only on the immediate consequences, as opposed to a defined long-term outcome, can be described as single-loop learning. Single-loop learning is not sufficient instead organizations should focus on double-loop learning (Malhotra, 1996, Rowe, 1996). Training program organizers for organizational learning efforts have to set programme objectives and, on the basis of this, plan, implement, and review a program (Rowe, 1996).

Thirdly, evaluation, or assessment, is critical to all three these models. According to the NIST model evaluation is the only way to ensure that training efforts is meaningful (NIST, 1998, p.155). OBE requires continuous and constructive feedback to learners, without which learning cannot take place (Fingar, 1996;DOE, 2001). Lastly, Organizational learning requires an evaluation of the consequences of actions. Without such an evaluation, the "mind maps" determining action strategies cannot be adapted. Thus no learning can take place without evaluation of some form.

Fourthly, learners must know **why** they should behave in a certain way or follow a specific policy. The NIST model reserves this level, where learners are taught why for information security specialist. But, according to NIST (1998, p.20) 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). Therefore it is imperative for learners to know why they are learning something (Schlienger & Teufel, 2003). 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. Double-loop learning does not directly require learners to know why they are taught something. But it does require the governing variables to be re-examined if the desired consequences has not been reached. Which, in turn, can be construed as knowing why a specific action strategy is taught.

Lastly, learning material should be customized for individual learners. The NIST model is role-based. The specific training needs of individuals should be identified based on their role within the organization. Specifically, training is to be provided to individuals based on their particular job functions (NIST, 1998, p. 43). Furthermore, 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). 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.

6 CONCLUSION

According to Siponen (2001), most current user education programs fail to pay adequate attention to behavioral theories. Since the emphasis of user education programs should be to build an organizational sub-culture of security awareness (Von Solms, 2000), the programs used to educate users should be suitable for modifying user behaviour. This paper examined three pedagogical models that are based on behavioural theories and attempted to identify common characteristics between these models. The aim of this paper is not to provide a complete solution to current problems with information security education, but rather to introduce some elements that could improve the effectiveness of such programs. The following key elements, that should be considered when constructing programs aimed at modifying employee behaviour, have been identified:

- Programs should be thoroughly planned using a formalised methodology, which takes into consideration aspects relating to both the learners and the environment in which they operate.
- Programs should be designed around a clearly defined outcome or goal, in terms of the desired results, for example: the desired change in employee behaviour.
- Evaluation, or assessment, is critical for the success of a learning program. Learners **must** receive feedback if learning is supposed to take place.
- Learners must not only be taught how to behave in a specific situation but should also be taught **why** they should behave in that specific way.
- Learning materials should be customized to individual learners

A lot of additional research would be required in order to provide a complete solution to all current information security education problems. For example, the link between the establishment of an information security culture and double-loop learning, which requires one to re-examine, and possibly modify, the underlying governing variables, warrants further investigation. This paper only examined the common characteristics of the three models. Furthermore, it only focused on "positive" aspects of these models. Future research should also include an examination of the weaknesses of each approach. Many other models for information security education exist. A rigorous scientific examination of such models, dealing with both common elements and weaknesses, would be very beneficial. However, any additional research would have to take into account both the goal of a user education program, to help establish a culture of information security awareness, and sound pedagogical principles.

7 REFERENCES

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

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

Horrocks, I. (2001). "Security Training: Education For an Emerging Profession?" Computers & Security 20(3): 219-226.

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.

Malhotra, Y. (1996) Organizational Learning and Learning Organizations: An Overview [WWW document]. URL http://www.brint.com/papers/orglrng.htm. Sited 4 March 2004.

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.

Rowe, C. (1996) Evaluating management training and development: revisiting the basic issues. Industrial and Commercial Training, 28 (4), Pp. 17-23.

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.

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

Siponen, M.T. (2000) A Conceptual Foundation for Organizational Information Security Awareness. Information Management & Computer Security. 8 (1), pp. 31-41.

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

Smith, M., K. (2001:1). Chris Argyris: Theories of action, double-loop learning and organizational learning. [WWW document]. URL http://www.infed.org/thinkers/argyris.htm. Sited 4 March 2004.

Smith, M., K. (2001:2). Donald Schon: Learning, Reflection and change. [WWW document]. URL http://www.infed.org/thinkers/et-schon.htm. Sited 4 March 2004.

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.

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.

ACKNOWLEDGEMENTS

The financial assistance of 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.