BLOOM'S TAXONOMY FOR INFORMATION SECURITY EDUCATION

Johan van Niekerk[1], Rossouw von Solms[2]

**[1]Nelson Mandela Metropolitan University
South Africa
[2]Nelson Mandela Metropolitan University
South Africa**

[1]johan.vanniekerk@nmmu.ac.za, [2]rossouw.vonsolms@nmmu.ac.za

ABSTRACT

The importance of educating organizational end users about their roles and responsibilities towards information security is widely acknowledged. However, many current user education programs have been created by security professionals who do not necessarily have an educational background. The nature of such programs is thus not always properly understood. This lack of understanding could result in the ineffectiveness of security guidelines or programs in practice. This paper attempts to provide additional understanding of these programs through an examination of the revised version of Bloom's taxonomy. The paper show how this taxonomy could be applied to information security education.

KEY WORDS

Information Security, Information Security Education, Awareness, Bloom's Taxonomy

BLOOM'S TAXONOMY FOR INFORMATION SECURITY EDUCATION

1 INTRODUCTION

In recent years information technology has become such an intrinsic part of modern business that some authors no longer see the use of information technology as a strategic benefit. Instead, it can be argued that information technology is a basic commodity, similar to electricity, and that the lack of this commodity makes it **impossible** to conduct business (Carr, 2003). It is therefor vital for organizations to ensure that they have continuous access to this valuable commodity. The process of ensuring this continuous access is known as information security.

Humans, at various levels in the organization, play a vital role in the processes that secures organizational information resources. Many of the problems experienced in information security can be directly contributed to the humans involved in the process. Employees, either intentionally or through negligence, often due to a lack of knowledge, can be seen as the greatest threat to information security (Mitnick & Simon, 2002, p. 3). It is thus imperative for organizations that are serious about the protection of its information resources to be serious about the education of its employees. The aim of corporate information security education should be to ensure that each and every employee in the organization knows his/her responsibility towards information security.

This need to educate organizational users about their roles and responsibilities towards information security is in fact a well established idea. Most major information security standards address this need in some form. For example, the ISO/IEC standard 13335-1 states that organizations cannot protect the integrity, confidentiality, and availability of information in today's highly networked systems environment without ensuring that each person involved shares the security vision of the organization, understands his/her roles and responsibilities, and is adequately trained to perform them (ISO/IEC TR 13335-1, 2004, p. 14). In order to assist in ensuring information security, individual users thus needs **knowledge** regarding their specific role in the security process. This knowledge can be provided via education, training and awareness campaigns.

Most current information security educational programs are constructed by information security specialists who do not necessarily have a strong educational background. Puhakainen (2006, pp. 33-56) reviews 59 current approaches to security awareness, most of which are not based on pedagogical theories. Puhakainen (2006, p. 56) also argues that there is a need for theory-based security approaches. These approaches should also be practically effective. The nature of security educational or awareness issues are often not understood, which could lead to programs and guidelines that are ineffective in practice (Siponen, 2000). A formally trained educationalist might, for example, raise the question whether or not **knowledge** is in fact enough. In Bloom's taxonomy, which is a well know and widely accepted pedagogical taxonomy, knowledge only comprises the very first, and lowest, level of education (Sousa, 2006, pp. 248-255). One could argue that this level of comprehension is in fact not adequate for most humans who play a role in the information security process. Similarly, the traditional approach of classifying the requisite information security educational needs as a continuum consisting of either awareness, training or education, might also be too simplistic.

This paper will attempt to provide a more pedagogically sound interpretation of the educational needs of humans involved in information security processes, based on their respective roles and responsibilities towards security, through the incorporation of Bloom's revised taxonomy (Anderson et al., 2001) as a pedagogical framework.

2 RESEARCH PARADIGM AND RATIONALE

The work in this paper is based on qualitative, or phenomenological-, research methods, as described in Creswell (1998). This paper should thus be seen as "an inquiry process of understanding based on distinct methodological traditions of inquiry that explore a social or human problem" (Creswell, 1998, p. 15). The research presented here does not attempt to define *new* knowledge, but rather to provide a more formalized understanding of information security *awareness*, *training* and *education*. As far as could be determined, the application of Bloom's Taxonomy, both the original and the revised versions, specifically to *information security* education has never been published before. It is the authors' belief that the use of this taxonomy could improve the understanding of the pedagogical issues that **should** be considered in any educational program, amongst information security specialists.

Since education, as a field of study, is normally seen as a ""human science" it was deemed fitting to also "borrow" the research paradigm used in this paper from the humanities. Most current work dealing with information security education see this education as a continuum consisting of three main levels, namely; awareness, training and education (Schlienger & Teufel, 2003),(Van Niekerk & Von Solms, 2004),(NIST 800-16, 1998, pp. 15-17). This continuum is used by many information security specialists when constructing information security educational campaigns. These specialists may not necessarily be educationalists. In order to ensure a rigorous research approach, this paper will thus revisit even concepts with a seemingly obvious meaning. The description and discussion of these concepts is deemed necessary because there might exist differences between the ontologies commonly adhered to by information security specialists and researchers from the educational sciences. The primary purpose of this paper is to encourage information security specialists to "borrow" from the humanities when engaged in activities that deals with humans. It can be argued that for most security education programs more knowledge of the underlying theoretical background can help both practitioners and scholars to understand why a particular information security awareness approach is expected to have the desired impact on users security behavior (Puhakainen, 2006, p. 139). It is believed that adherence to sound pedagogical principles when constructing information security educational campaigns, could improve the efficiency of such campaigns.

3 AWARENESS, TRAINING AND EDUCATION

As mentioned earlier, most current work dealing with information security education see this education as a learning continuum that "starts with awareness, builds to training, and evolves into education" (NIST 800-50, 2003, p. 7). NIST 800-16 (1998, pp. 15-17) provides more detail on the various levels of this continuum and describes these levels as follow:

- Awareness: The main purpose of awareness campaigns is to make employees "*aware*" of information security. In other words, these campaigns focus attention on security. This is normally done using techniques that can reach broad audiences. Awareness campaigns are generally aimed at **all** employees in the organization and aims to equip employees with enough knowledge to enable them to recognize potential security threats. Awareness is not training.

- Training: Training is more formal than awareness and have the goal of building employee knowledge and skills to facilitate the *secure* performance of the employee's normal tasks. Training strives to produce security skills and competencies that are relevant to the specific employee and needed in the performance of the employee's duties. "The most significant difference between training and awareness is that training seeks to teach skills that allow a person to perform a specific function, while awareness seeks to focus an individuals attention on an issue or set of issues."

- Education: "The Education level integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge, adds a multi-disciplinary study of concepts, issues, and principles (technological and social), and strives to produce IT security specialists and professionals capable of vision and pro-active response."

In the current information society, educational or awareness issues affect almost all organizations. Despite this fact the nature of these programs are still not well understood and this often leads to ineffective security guidelines or programs (Siponen, 2000). Many organizations have some form of *awareness* program but often do not augment these with supporting training and/or education programs. The terms *awareness* and *education* are also often used interchangeably. It is not uncommon to hear security specialists talk about "awareness campaigns", when the campaigns actually focus on the training or education levels of the continuum. The purpose of these campaigns is often listed as instilling security **knowledge**, or fostering a **culture** of information security amongst organizational end-users (Van Niekerk & Von Solms, 2006). As mentioned earlier, the term knowledge only describe the lowest level of Bloom's taxonomy of the cognitive domain. From an educational viewpoint one could thus argue that the terminology used lacks rigor. This lack of rigor could contribute to the fact that the nature of awareness and educational issues is often misunderstood. One model that could possibly provide such rigor is Bloom's taxonomy.

4 BLOOM'S TAXONOMY OF THE COGNITIVE DOMAIN

Bloom's taxonomy is possibly one of the best known and most widely used models of human cognitive processes. Bloom's model was originally developed in the 1950's and remained in use more or less unchanged until fairly recently (Sousa, 2006, p. 249). A revised version of the taxonomy was published in Anderson et al. (2001). This revised taxonomy has become accepted as more appropriate in terms of current educational thinking (Sousa, 2006, pp. 249-260). Both versions of Bloom's taxonomy consist of six levels which increases in complexity as the learner moves up through these levels. Figure 1 shows both versions of this taxonomy.

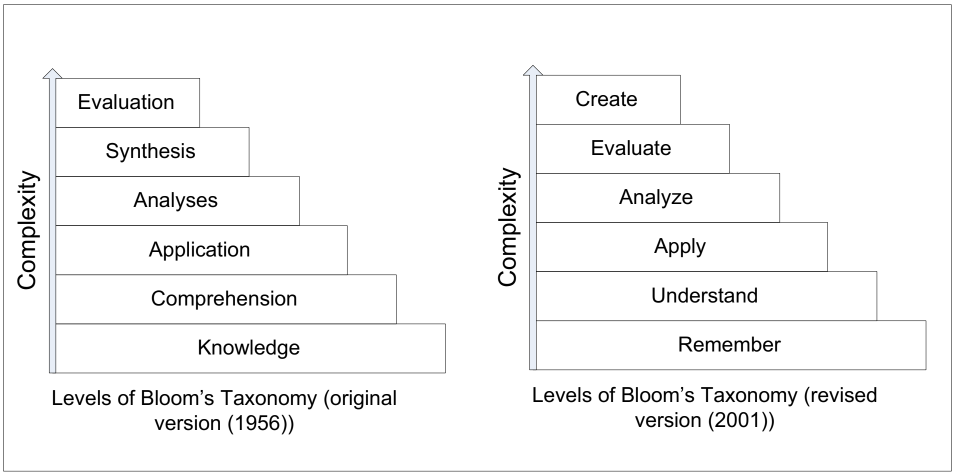

Figure 1: Blooms Taxonomy, Original and Revised (Adapted from Sousa (2006) pp. 249-250)

There are two main differences between the original and the revised versions of the taxonomy. Firstly, the revised version uses descriptive verbs for each level that more accurately describes the intended meaning of each level. Secondly, the revised version has swapped the last two levels of the original version around. This was done because recent studies have suggested that generating, planning, and producing an original "product" demands more complex thinking than making judgements based on accepted criteria (Sousa, 2006, p. 250). The hierarchy of complexity in the revised taxonomy is also less rigid than in the original in that it recognizes that an individual may move among the levels during extended cognitive processes. This paper will focus on the revised version of the taxonomy. Wherever this paper mentions Bloom's taxonomy, it should be assumed that the revised version is intended, unless otherwise stated. The following is a brief explanation of each of the six levels of this revised taxonomy (Sousa, 2006, pp. 250-252):

- Remember: Remember refers to the rote recall and recognition of previously learned facts. This level represents the lowest level of learning in the cognitive domain because there is no presumption that the learner understands what is being recalled.

- Understand: This level describes the ability to "make sense" of the material. In this case the learning goes beyond rote recall. If a learner understands material it becomes available to that learner for future use in problem solving and decision making.

- Apply: The third level builds on the second one by adding the ability to use learned materials in *new* situations with a minimum of direction. This includes the application of rules, concepts, methods and theories to solve problems within the given domain. This level combines the activation of procedural memory and convergent thinking to correctly select and apply knowledge to a completely new task. Practice is essential in order to achieve this level of learning.

- Analyze: This is the ability to break up complex concepts into simpler component parts in order to better understand its structure. Analysis skills includes the ability to recognize underlying parts of a complex system and examining the relationships between these parts and the whole. This stage is considered more complex than the third because the learner has to be aware of the thought process in use and must understand both the content and the structure of material.

- Evaluate: Evaluation deals with the ability to judge the value of something based on specified criteria and standards. These criteria and/or standards might be determined by the learner or might be given to the learner. This is a high level of cognition because it requires elements from several other levels to be used in conjunction with conscious judgement based on definite criteria. To attain this level a learner needs to consolidate their thinking and should also be more receptive to alternative points of view.

- Create: This is the highest level in the taxonomy and refers to the ability to put various parts together in order to formulate an idea or plan that is new to the learner. This level stresses creativity and the ability to form *new* patterns or structures by using divergent thinking processes.

Educational taxonomies, such as Bloom's taxonomy, are useful tools in developing learning objectives and assessing learner attainment (Fuller et al., 2007). All well known educational taxonomies are generic. These taxonomies rely on the assumption that the hierarchy of learning outcomes apply to all disciplines (Fuller et al., 2007). Bloom's taxonomy would thus apply equally to a more traditional ”subject”, such as zoology, as to organizational information security education.

5 BLOOM'S TAXONOMY FOR INFORMATION SECURITY EDUCATION

Learning taxonomies assist the educationalist to describe and categorize the stages in cognitive, affective and other dimensions, in which an individual operates as part of the learning process. In simpler terms one could say that learning taxonomies help us to ”understand about understanding” (Fuller et al., 2007). It is this level of meta-cognition that is often missing in information security education. According to Siponen (2000) awareness and educational campaigns can be broadly described by two categories, namely framework and content. The framework category contains issues that can be approached in a structural and quantitative manner. These issues constitute the more explicit knowledge. The second category, however, includes more tacit knowledge of an interdisciplinary nature. Shortcomings in this second area usually invalidate awareness frameworks (Siponen, 2000). How to really motivate users to adhere to security guidelines, for example, is an issue that would form part of this content category.

It has been shown that even in cases where users have ”knowledge” of a specific security policy, they might still willfully ignore this policy because they do not understand *why* this policy is needed (Schlienger & Teufel, 2003). Answering the question ”why” not only increase insight but also increases motivation (Siponen, 2000). Simply informing employees that ”this is our policy”, or ”you just have to do it”, which is often the traditional approach, is not likely to increase motivation or attitudes (Siponen, 2000). Learning is a willful, active, conscious, and constructive activity guided by intentions and reflections (Garde et al., 2007). According to most constructivist learning theories, learning should be learner-centered (Garde et al., 2007). In an organizational information security educational campaign, the learners **must** include each and every employee. It is also important to realize that the campaign has to be **successful for each and every learner** (Van Niekerk & Von Solms, 2004).

In order to ensure successful learning amongst all employees, it is extremely important to fully understand the educational needs of individual employees. According to Roper, Grau, and Fischer (2005, pp. 27-36) managers often attempt to address the security education needs of employees without adequately studying and understanding the underlying factors that contribute to those needs. It has been argued before that educational material should ideally be tailored to the learning needs and learning styles of individual learners (Van Niekerk & Von Solms, 2004)(NIST 800-16, 1998, p. 19). One could also argue that awareness campaigns that have not been tailored to the **specific** needs of an individual, or the needs of a **specific target audience**, will be ineffective. It is in the understanding of these needs, that a learning taxonomy can play an important enabling role.

Information security specialists should use a taxonomy, like Bloom's taxonomy, before compiling the content category of the educational campaign. The use of such a taxonomy could help to understand the learning needs of the target audience better. It could also reduce the tendency to focus only on the framework category of these campaigns. For example, simply teaching an individual what a password is, would lie on the *remember*, and possibly *understand* level(s) of Bloom's taxonomy. However, the necessary information to understand *why* their own passwords is also important and should also be properly constructed and guarded might lie as high as the *evaluate* level of the taxonomy. An information security specialist might think that teaching the users what a password is, is enough, but research have shown that understanding *why* is essential to obtaining buy-in from employees. It is this level of understanding that acts as a motivating factor and thus enables behaviour change (Siponen, 2000)(Schlienger & Teufel, 2003)(Van Niekerk & Von Solms, 2004)(Roper et al., 2005, pp. 78-79).

The use of an educational taxonomy in the construction of information security educational programs requires that both the content and the assessment criteria for this program is evaluated against the taxonomy in order to ensure that learning takes place at the correct level of the cognitive do-

Level	**Terms**	**Sample Activities**
Create	imagine	Pretend you are an information security officer for a large firm. Write a report about a recent security incident.
	compose	Rewrite a given incident report as a news story.
	design	Write a new policy item to prevent users from putting sensitive information on mobile devices.
	infer	Formulate a theory to explain why employees still write down their passwords.
Evaluate	appraise	Which of the following policy items would be more appropriate. Why?
	assess	Is it fair for a company to insist that employees never use their work email for personal matters? Why or Why not?
	judge	Which of the security standards you have studied is more appropriate for use in the South African context? Defend your answer.
	critique	Critique these two security products and explain why you would recommend one over the other to a customer.
Analyze	analyze	Which of the following security incidents are more likely?
	contrast	Compare and contrast the security needs of banking institutions to those of manufacturing concerns.
	distinguish	Sort these security controls according to the high level policies that they address.
	deduce	Which of these procedures could derive from the given policy.
Apply	practice	Use these mnemonic techniques to create and recall a secure password.
	calculate	Calculate how secure the following password is.
	apply	Think of three things that could go wrong should your password be compromised.
	execute	Use the given tool to encrypt the following message.
Understand	summarize	Summarize the given security policy in your own words
	discuss	Why should non alpha-numeric characters be used in a password?
	explain	Explain how symmetric encryption works.
	outline	Outline your own responsibilities with regards to the security of customer account information.
Remember	define	What is the definition of a security incident?
	label	Label each of the threats in the given picture.
	recall	What is social engineering?
	recognize	Which of the pictures shows someone ”shoulder surfing”?

Table 1: Bloom’s Taxonomy for Information Security adapted from Anderson et al., 2001

main. The reference point for any educational program should be a set of clearly articulated "performance objectives" that have been developed based on an assessment of the target audience's needs and requirements (Roper et al., 2005, p. 96). Correct usage of an educational taxonomy not only helps to articulate such performance objectives but, more importantly, helps the educator to correctly gauge the needs and requirements of the audience. An example of how Bloom's revised taxonomy could be used in an information security context is supplied in Table 1. This example is not intended to be a definitive work, but rather to serve as an example or starting point for information security practitioners who want to use Bloom's taxonomy when constructing awareness and educational campaigns. It should however be clear that this taxonomy could easily be used to categorize most, if not all, information security educational needs effectively. Once categorized according to a taxonomy like Bloom's taxonomy, it should also be easier to find related information regarding pedagogical methods suitable to assist learners in attaining the desired level of cognitive understanding.

6 CONCLUSION

This paper suggested that information security educational programs would be more effective if they adhered to pedagogical principles. It was specifically suggested that the common categorization of security educational needs into the broad categories of awareness, training, and education, is not ideal. Instead an educational taxonomy, like Bloom's taxonomy should be used to accurately define the security education needs of organizational users. Through the use of such a taxonomy certain common weaknesses in current security awareness and educational programs might be addressed.

An example of how Bloom's taxonomy might be applied to information security concepts was provided. The primary weakness of this paper is the lack of empirical evidence to support the suggested use of Bloom's taxonomy. Future research in this regard should therefor focus on addressing this weakness. It has been argued before that security practitioners who engage in research or activities that relate to the human sciences should not re-invent the wheel, but should rather "borrow" from the humanities when appropriate. This paper is one such an attempt, to "borrow" from the humanities.

References

Anderson, L., Krathwohl, D., Airasian, P., Cruikshank, K., Mayer, R., Pintrich, P., et al. (2001). *A taxonomy for learning, teaching, and assessing: A revision of bloom's taxonomy of educational objectives, complete edition* (L. Anderson & D. Krathwohl, Eds.). Longman.

Carr, N. G. (2003). IT Doesn't Matter. *Harvard Business Review*, 41–49.

Creswell, J. W. (1998). *Qualitative inquiry and research design: Choosing among five traditions. thousand oaks, ca: Sage, 1998.* Thousand Oaks, CA: Sage.

Fuller, U., Johnson, C. G., Ahoniemi, T., Cukierman, D., Hernán-Losada, I., Jackova, J., et al. (2007). Developing a computer science-specific learning taxonomy. *SIGCSE Bull.*, *39*(4), 152–170.

Garde, S., Heid, J., Haag, M., Bauch, M., Weires, T., & Leven, F. J. (2007). Can design principles of traditional learning theories be fullfilled by computer-based training systems in medicine: The example of campus. *International Journal of Medical Informatics*, *76*, 124–129.

International Standards Organization. (2004). *ISO/IEC TR 13335-1:2004 Guidelines to the Management of Information Technology Security (GMITS). Part1: Concepts and models for IT security. ISO/IEC, JTC 1, SC27, WG 1.*

Mitnick, K., & Simon, W. (2002). *The art of deception: Controlling the human element of security.* Wiley Publishing.

National Institute of Standards and Technology. (1998). *NIST 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model. NIST Special Publication 800-16, National Institute of Standards and Technology.*

National Institute of Standards and Technology. (2003). *NIST 800-50: Building an Information Technology Security Awareness and Training Program. NIST Special Publication 800-50, National Institute of Standards and Technology.*

Puhakainen, P. (2006). *A design theory for information security awareness.* Unpublished doctoral dissertation, Acta Universitatis Ouluensis A 463, The University of Oulu.

Roper, C., Grau, J., & Fischer, L. (2005). *Security Education, Awareness and Training: From Theory to Practice.* Elsevier Butterworth Heinemann.

Schlienger, T., & Teufel, S. (2003). Information security culture - from analysis to change. *Information Security South Africa (ISSA), Johannesburg, South Africa.*

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Sousa, D. A. (2006). *How the brain learns* (3rd ed.). Corwin Press.

Van Niekerk, J., & Von Solms, R. (2004). Corporate information security education: Is outcomes based education the solution? *10th IFIP WG11.1 Annual Working Conference on Information Security Management, World Computer Congress (WCC), Toulouse, France.*

Van Niekerk, J., & Von Solms, R. (2006). Understanding information security culture: A conceptual framework. *Information Security South Africa (ISSA), Johannesburg, South Africa.*

7 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.