Evaluating the Cisco Networking Academy Program's Instructional Model against Bloom's Taxonomy for the purpose of Information Security Education for Organizational End-users

J. F. Van Niekerk, K. Thomson

Evaluating the Cisco Networking Academy Program's Instructional Model against Bloom's Taxonomy for the purpose of Information Security Education for Organizational End-users

J.F. van Niekerk[1], K Thomson[1],

[1] Institute for ICT Advancement
Nelson Mandela Metropolitan University
{Johan.vanniekerk,Kerry-Lynn.Thomson
}@nmmu.ac.za

Abstract. Organizational end-user information security end-user education is becoming increasingly more important in the current *information society*. Without the active co-operation of *knowledgeable* employees, organizations cannot effectively protect their valuable information resources. Most current information security educational programs lack a theoretical basis. This paper briefly examines the use of Bloom's learning taxonomy to help address this lack of theoretical basis. The paper further investigates the applicability of the Cisco Networking Academy Program's (CNAP) instructional model for the delivery of end-user information security instructional content, planned with the assistance of Bloom's taxonomy.

Keywords: Information Security Education, Bloom’s Taxonomy, Blended Learning, E-learning

1 Introduction

According to Carr [1] the dependency on information technology has become so great that it should no longer be viewed as conveying a competitive advantage, but rather as a basic commodity, similar to electricity. Unfortunately, the availability of one's information is often a lot more vulnerable than the availability of other commodities. Without adequate protection, information resources are extremely vulnerable. It is thus vital for organizations to be serious about the protection of information resources.

Humans, at various levels in the organization, play a vital role in the processes that secure 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 [2, 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 end-user education should be to ensure that each and every employee in the organization knows his/her responsibility towards information security.

Most current information security end-user educational programs are constructed by information security specialists who do not necessarily have a strong educational background. Puhakainen [3, pp. 33-56] reviews 59 current approaches to security awareness, most of which are not based on pedagogical theories. Puhakainen [3, 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 [4]. One possible way to introduce pedagogical theory as a basis for information security awareness programs is through the use of learning taxonomies. Arguably the most widely used of these learning taxonomies is Bloom's taxonomy of the cognitive domain.

Previous papers have shown how Bloom's taxonomy could be used in information security end-user education. Van Niekerk & Von Solms [5] argued that Bloom's taxonomy of the cognitive domain can be used as a theoretical basis to partly ensure the pedagogical integrity of information security awareness programs. Van Niekerk & Von Solms [6] showed how the use of this taxonomy could help information security specialists to answer the four so-called organizing questions when creating awareness programs. The use of Bloom's taxonomy during the creation of information security educational material could thus assist in ensuring that; the most important learning activities receive the larger share of available resources (learning question), the instructional material is planned around activities that will benefit most learners (instruction question), the chosen assessments correspond directly to what the educator intended to assess (assessment question), and that all activities align towards the intended learning outcomes (alignment question) [7, pp. 6-10].

Through the use of a learning taxonomy information security practitioners can plan what to include in information security educational programs. However, another equally important question still needs to be addressed. Namely, how the content should be delivered. Few, if any, modern organizations can afford to send each and every staff member on extensive information security educational courses. 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 alternative to traditional classroom training is to provide employees with E-learning alternatives.

E-learning has been used with great effect in other information technology related fields. For example, the Cisco Networking Academy Program (CNAP) plays a widely recognized role in the education of networking professionals. This program is based on a blended learning approach, which combines E-learning, classroom instruction and hands-on practical work as part of a wide spectrum of teaching and assessment approaches. This paper will evaluate the instructional model used by CNAP against the requirements for a learning program designed according to Bloom's taxonomy. The purpose of this evaluation is to determine whether the CNAP instructional model would meet all the requirements for educating end users about information security.

The rest of this paper will firstly discuss E-learning and blended learning in general in order to demonstrate the suitability of these types of instructional programs for the specific needs of information security end-user education. Secondly, a brief outline of the CNAP instructional model will be provided and the paper will then discuss how Bloom's taxonomy can be used in information security education. Finally a comparative analysis will be done to demonstrate how well the CNAP instructional model maps to the educational requirements of a pedagogically sound end-user information security educational program.

2 Why Blended and/or E-learning?

In an organizational context, information security end-user education has several requirements specific to the role that such programs have to play in the overall organization's information security efforts. Van Niekerk & Von Solms [8] identified these requirements and discussed the pedagogical implications of these requirements in depth. The following is a brief summary of the identified requirements:

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

It can be argued that, in terms of the above requirements, e-learning solutions are ideally suited to the needs of information security end-user education. E-learning based training solutions have several benefits over more traditional approaches like classroom training. These benefits include:

- Electronic and/or web-based media is very rich. This means that educational material developed in these types of media is not restricted to simple text and static graphics, but can consist of a mixture of text, graphics, animations and even sound or video clips.
- E-learning based training solutions are inexpensive to distribute organization wide and can easily be administrated from a centralized point. This also means that it would be very easy to maintain, manage and update training materials.
- E-learning training materials can include programmatic components, which could allow virtually limitless customization.

The fact that web-based training materials can include programmatic components has several important implications for its possible use in information security end-user education. Firstly, it would make it feasible to add automated assessment modules to such training materials, which means that learners can receive continuous feedback on their progress. Automated feedback, in combination with the fact that this material would be available at all times, means that learners could be made responsible for their own learning. Automated assessment would also enable organizations to hold learners accountable for their own learning. The use of automated assessment also makes it easier to allow users multiple attempts at passing specific assessments modules. This can contribute to an environment where everyone could eventually "pass" the course.

The U.S. Department of Education published a report based on a meta-analysis of the results of more than 1000 empirical studies that were published from 1996 through July 2008 [9]. The report focused predominantly on publications after 2004 which compared the effectiveness of various forms of e-learning and blended learning to face-to-face education [9, p. xiii]. This report examined 51 identified study effects, of which 44 were drawn from research focusing on older (adult) learners. This focus on older learners is of particular importance to educators focusing on organizational information security end-user education who work exclusively with adult learners. Adults already 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 [10, p. 20]. It is therefore vital to ensure that learning approaches followed are suitable for adult learners. The fact that 44 of the 51 study effects analyzed in the meta-analysis focus on adult learners makes the results of this analysis very relevant. The following key-findings are of specific importance for the purposes of this paper [9, p. xiv-xvi]:

- "Students who took all or part of their class online performed better, on average, than those taking the same course through traditional face-to-face instruction"
- "Instruction combining online and face-to-face elements had a larger advantage relative to purely face-to-face instruction than did purely online instruction"
- "The effectiveness of online learning approaches appears quite broad across different content and learner types."

These findings make it clear that a blended or e-learning approach would not only be effective for information security end-user education, but would in fact be better than traditional face-to-face education. "A blended approach" would thus answer the question "How should educational content be delivered?". However, the question "what should be taught to organizational end-users?" still remains. The use of a learning taxonomy might assist in answering this question.

3 Bloom's Taxonomy

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 1950s and remained in use more or less unchanged until fairly recently [11, p. 249]. A revised version of the taxonomy was published in [7]. This revised taxonomy has become accepted as more appropriate in terms of current educational thinking [11, pp. 249-260]. The following is a brief explanation of each of the six levels of the revised taxonomy [11, 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 include the ability to recognize underlying parts of a complex system and examine the relationships between these parts and the whole. This stage is considered more complex than the previous 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 [12]. All well known educational taxonomies are generic. These taxonomies rely on the assumption that the hierarchy of learning outcomes apply to all disciplines [12]. Bloom's taxonomy would thus apply equally to a more traditional "subject", such as zoology, as to organizational information security end-user education. In addition to these levels of the cognitive domain the revised taxonomy also places major emphasis on the use of the following categorization of the knowledge dimension [7, pp. 45-62]:

- *Factual Knowledge* - The most basic elements the learner must know in order to be familiar with a discipline. I.e. Terminology or specific details and elements.
- *Conceptual Knowledge* - The interrelationships among the basic elements of larger structures that enable these elements to function together. I.e. Classification, categories, principles, theories, models, etc.
- *Procedural Knowledge* - How to do something, methods of inquiry, how to use skills, apply algorithms, techniques and methods. I.e. Subject specific skills, algorithms, techniques, and methods as well as knowledge of criteria for determining when to use appropriate procedures.

- *Meta-Cognitive Knowledge* - An awareness and knowledge of one's own cognition. I.e. Strategic knowledge, Self-knowledge, knowledge about cognitive tasks, including contextual and conditional knowledge.

The use of this taxonomy for information security end-user education will be discussed in a later section of this paper. The next section will briefly outline the instructional model used by the Cisco Networking Academy Program.

4 The Cisco Networking Academy Program instructional model

The Cisco Networking Academy Program (CNAP) is a global e-learning education program that teaches students to design, troubleshoot and secure communication networks. Core to CNAP is the Learning Management System. Through the Learning Management System, referred to as the Instructor Portal in CNAP, instructors are able to create online classes, enroll students and activate assessments. The progress of each student can be monitored through an online *Gradebook*. In addition, many tools and teaching guidelines are provided through the online management system to assist instructors in teaching.

Further to the Learning Management System, there are six key components that contribute to the blended learning in CNAP:

1. *Instructor-led Lessons* All CNAP instructors receive extensive training and employ traditional teaching methods to educate students, facilitate discussion, workshops and lectures.
2. *Online Learning Curricula* The CNAP curricula are available online through the Academy website or are hosted on a local server. The CNAP material is divided into Chapters by topic and when the online CNAP material is opened by the students, they are able to choose which topic to study by selecting a Chapter. The online material is extremely feature rich and includes many graphics, animations, quizzes and activities which allow students to gain immediate feedback on the knowledge acquired throughout the Chapter. Further to this, there are many web links that assist those students who would like a deeper understanding of a particular topic by guiding them to relevant websites.
3. *Self-paced Lessons* The CNAP curricula are always available online or on a local server. This allows each student to study the material at his/her own pace, which is further facilitated through e-learning techniques, as discussed in the previous sub-section.
4. *Glossary/Course Index* Each Chapter contains a Course Index, which enables easy navigation of the material, a Glossary, for referencing definitions of terms and a Search feature.
5. *Practical Lab Work* Much of the CNAP material is communicated to students through Practical Lab Work using a combination of hands-on practical activities and network simulations. Each Chapter in the Cisco curricula has related practical activities and simulations which are conducted on laboratory equipment.

6. *Assessments* For students to pass a particular class, they must pass two Final Assessments, namely; the Online Final Exam and the Practical Skills Exam. To assist students in preparation for these exams, at the end of each Chapter, students are able to test their knowledge through online Chapter exams and quizzes.

CNAP is one of the most comprehensive and widely used blended learning programs in the world. The use of its instructional model could potentially address many issues relating to the delivery and administration of information security end-user education. In order to design the learning program content in information security programs, the use of a learning taxonomy could be of assistance.

5 Using Bloom's taxonomy

As described earlier, Bloom's taxonomy consists of six levels of the cognitive domain and is further divided into four categories of knowledge. Activities at the six levels of the cognitive domain are usually combined with one or more of the four types of knowledge in a collection of statements outlining the learning objectives of an educational program. Usually a learning objective statement will be used to create a set of learning activities. Learning activities are activities which help learners to attain the learning objectives. A learning activity consists of a verb that relates to an activity at one of the levels of the cognitive domain, and a noun providing additional insight into the relationship of the specific learning objective to a category of knowledge [7, pp. 93-109].

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" [12]. It is this level of meta-cognition that is often missing in information security end-user education.

5.1 Bloom's Taxonomy for information security end-user education

Bloom's Taxonomy for information security end-user education. According to Siponen [4] awareness and educational campaigns can be broadly described by two categories, namely framework and content [4]. 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 [4]. *How to really motivate users to adhere to security guidelines*, for example, is an issue that would form part of this content category.

In order to ensure successful learning amongst all employees, it is extremely important to fully understand the educational needs of individual employees. Managers often attempt to address the security education needs of employees without adequately studying and understanding the underlying factors that contribute to those needs [13, pp. 27-36]. It has been argued before that educational material should ideally be tailored to the learning needs and learning styles of individual learners [8][10, 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 are also important and should 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, would be enough, but research has 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 [4][8][13, pp. 78-79].

Table 1. Abbreviated example of Learning Activities based on Bloom's Taxonomy for Information Security, adapted from [7].

Level	*Verb*	*Sample Activities*
Create	design	Write a new policy item to prevent users from putting sensitive information on mobile devices. *(IS-A6)*
Evaluate	critique	Critique these two passwords and explain why you would recommend one over the other in terms of the security it provides. *(IS-A5)*
Analyze	analyze	Which of the following security incidents involving stolen passwords are more likely in our company? *(IS-A4)*
Apply	execute	Use the appropriate application to change your password for the financial sub-system. *(IS-A3)*
Understand	discuss	Why should non alpha-numeric characters be used in a password? *(IS-A2)*
Remember	define	What is the definition of *access control*? *(IS-A1)*

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 domain. 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 [13, 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.

Table 2. Example Taxonomy Table adapted from [7].

The Knowledge Dimension	The Cognitive Process Domain					
	Remember	Understand	Apply	Analyze	Evaluate	Create
Factual Knowledge	*IS-A1* *CNAP-A1*				*IS-A6*	
Conceptual Knowledge		*IS-Test1A* *IS-A2* *CNAP-A2*		*IS-Test1B* *IS-A4*	*IS-A6*	
Procedural Knowledge			*IS-LO1* *IS-A3*		*IS-A6*	
Meta-Cognitive Knowledge				*IS-A5*		

This example contains learning activities for a learning objective ***(IS-LO1)*** that can be briefly expressed as: "Learners should be able to understand, construct and use passwords in the correct context". This example in Table 1 is not intended to be a definitive work, but rather to serve, with the taxonomy table, shown in Table 2, towards clarifying the use of Bloom's taxonomy in an information security context, for a more detailed discussion on this topic, please refer to Van Niekerk & Von Solms [6].

5.2 Evaluating the CNAP instructional model against Bloom's taxonomy

Table 3 provides an example of how learning activities in the CNAP curriculum could be categorized according to Bloom's taxonomy. This example is similar to the information security example provided in Table 1.

Starting from the lowest level of the taxonomy, the first example learning activity in the above example ***(CNAP-A1),*** which deals with students having to remember the definition of a converged information network, is very similar to the first learning activity ***(IS-A1)*** in Table 1. Both of these could be further classified as being Factual Knowledge and would thus be mapped to the same cell in Table 2. The same would be true for many different activities involving rote learning in the CNAP program. The CNAP learning model has also proven itself to be effective in both the conveying of this type of knowledge, as well as, the assessment of this kind of knowledge. CNAP learners are also able to complete self-assessment tests after completing the relevant online curriculum material. If one also considers the fact that the effectiveness of blended and e-learning was found to be "broad across different content and learner types." [9], the argument could be made that for information security related material developed to address learning needs at this level of Bloom's taxonomy, the CNAP instructional model should be equally effective.

Table 3. Abbreviated example of Learning Activities based on Bloom's Taxonomy for the Cisco Networking Academy Program, adapted from [7].

Level	*Verb*	*Sample Activities*
Create	design	Design a converged information network to meet the needs of Company A? ***(CNAP-A6)***
Evaluate	critique	Critique these two converged information network designs. Which would be best for Company A? ***(CNAP-A5)***
Analyze	analyze	Analyze the given design for a converged information network and determine whether it meets Company A's requirements? ***(CNAP-A4)***
Apply	execute	Implement a converged information network. ***(CNAP-A3)***
Understand	discuss	How does a converged information network differ from the traditional approach of separate networks? ***(CNAP-A2)***
Remember	define	What is the definition of a *converged information network*? ***(CNAP-A1)***

Similarly, the second example learning activity ***(CNAP-A2),*** which focuses on the understanding of a concept, can also be mapped to the same cell in Table 2 as the equivalent information security learning activity ***(IS-A2).*** Once again, the CNAP learning model would also be able to cater for the teaching of the information security learning activity at the second level of the cognitive domain. CNAP currently teaches similar concepts via the online curriculum and encourages understanding by allowing learners to explore concepts, interact with simulations, and answer self-evaluative assessments. In addition, learners in a blended environment will often be able to interact with an instructor via either face-to-face communication, or via some form of electronic medium, such as conference calls, e-mail, instant messaging, etc. Giving learners control of their interactions with media and prompting learner reflection, has been shown to enhance online learning [9, p. xvi].

For the purposes of this paper, demonstrating that all learning activities in CNAP could also be categorized according to Bloom's taxonomy is not necessary. However, it is the opinion of the authors' that it would be possible to express any of the current learning activities in CNAP according to Bloom's taxonomy. As mentioned earlier, learning taxonomies are not subject specific. The preceding examples simply serve to show how similar information security learning activities, as expressed using Bloom's taxonomy, are to examples of current learning activities in the CNAP curriculum. If one accepts the preceding argument that every activity currently in the CNAP curricula could be expressed using Bloom's taxonomy it could be argued that the CNAP instructional model has sufficient content delivery mechanisms to convey information at most, if not all, of the taxonomy's levels and knowledge categories. In addition the given examples serve to demonstrate that the CNAP instructional model could also accommodate the needs of information security learning activities. These needs will not necessarily always map to the exact same cell in Table 2 as the equivalent information security activity from Table 1, nor will they always be catered for by the exact same types of learning activities that teaches the CNAP activities at the same level of the cognitive domain. It should however be clear that the requirements, in terms of learning activities, of an information security end-user education program would be very similar to the requirements of a typical learning module in the CNAP program. In fact it could be argued that the learning requirements for a typical information security end-user would mostly be at lower levels of the cognitive domain than the learning needs of an advanced networking professional.

Once again, this supports the argument that the CNAP instructional model has sufficient content delivery mechanisms to meet the requirements of an end user information security educational program specified according to Bloom's taxonomy. The CNAP instructional model, as a blended learning approach, also meets the other requirements of information security end-user education mentioned in section 2.

6 Conclusion

This paper demonstrated that a definite need for more theory based approaches exists amongst current information security end-user educational programs and that the use of a learning taxonomy could help in addressing this current lack. The use of Bloom's taxonomy of the cognitive domain as a tool to help determine the appropriate learning content for information security educational programs was briefly examined. However, knowing what to teach to a learner does not adequately address how this content should be delivered to the intended learners.

This paper presented the argument that an e-learning or a blended learning approach to delivering organizational information security end-user education would be ideally suited to the specific requirements of organizational end-user information security education. The Cisco Networking Academy Program (CNAP) was then discussed as an ideal current example of such a blended learning approach. It was argued that the CNAP instructional model would in fact meet all the requirements of an information security end-user educational program and is also capable of delivering instructional content which was planned with the help of Bloom's taxonomy. If Bloom's taxonomy is used to determine what to teach to organizational end-users in an information security end-user education program, this paper has argued that a blended learning model similar to the one used by CNAP would be an appropriate answer to the question "how should the learning content be delivered to the intended audience?".

References

1. Carr, N.G.: IT Doesn't Matter. Harvard Business Review (2003) 41-49
2. Mitnick, K., Simon, W.: The art of deception: Controlling the human element of security. Wiley Publishing (2002)

3. Puhakainen, P.: A design theory for information security awareness. PhD thesis, Acta Universitatis Ouluensis A 463, The University of Oulu (2006)
4. Siponen, M.: A conceptual foundation for organizational information security awareness. Information Management & Computer Security 8(1) (2000) 31-41
5. Van Niekerk, J., Von Solms, R.: Bloom's taxonomy for information security education. Information Security South Africa (ISSA), Johannesburg, South Africa (2008)
6. Van Niekerk, J., Von Solms, R.: Using bloom's taxonomy for information security education. Education and Technology for a Better World. 9th IFIP TC 3 World Conference on Computers in Education, WCCE 2009, Bento Goncalves, Brazil, July 2009 (2009)
7. Anderson, L., Krathwohl, D., Airasian, P., Cruikshank, K., Mayer, R., Pintrich, P., Raths, J., Wittrock, M.: A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives, Complete Edition. Longman (2001)
8. Van Niekerk, J., Von Solms, R.: 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 (2004)
9. U.S. Department of Education: Office of Planning, Evaluation, and Policy Development Policy and Program Studies Service.: Evaluation of Evidence-Based Practices in Online Learning: A Meta-Analysis and Review of Online Learning Studies (2009)
10. National Institute of Standards and Technology: 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. (1998)
11. Sousa, D.A.: How the brain learns. 3rd edn. Corwin Press (2006)
12. Fuller, U., Johnson, C.G., Ahoniemi, T., Cukierman, D., Hern´an-Losada, I., Jackova, J., Lahtinen, E., Lewis, T.L., Thompson, D.M., Riedesel, C., Thompson, E.: Developing a computer science-specific learning taxonomy. SIGCSE Bull. 39(4) (2007) 152-170
13. Roper, C., Grau, J., Fischer, L.: Security Education, Awareness and Training: From Theory to Practice. Elsevier Butterworth Heinemann (2005)