Guidelines for the creation of brain-compatible cyber security educational material in Moodle 2.0

Rayne Reid
Institute for ICT Advancement
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
s208045820@live.nmmu.ac.za

Johan Van Niekerk
Institute for ICT Advancement
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
Johan.VanNiekerk@nmmu.ac.za

Rossouw Von Solms
Institute for ICT Advancement
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
Rossouw.VonSolms@nmmu.ac.za

Most current approaches towards information security education do not have a sound theoretical basis. This could lead to the failure of these educational programs. Furthermore, the need for information security knowledge is no longer only of concern to organizations, but has also become a concern for individuals using online services for personal entertainment, social networking, banking, and other activities. Thus, there is a need for "cyber security" education for both individuals and organizations. Such cyber security educational programs should be based on sound pedagogical theories. One such a pedagogically sound approach that could potentially play a role in cyber security educational programs is "brain compatible learning". This paper will perform a critical evaluation of an existing information security education course, and evaluate the subject matter in terms of brain compatible learning approaches. The aim of the paper is to propose a set of brain compatible learning guidelines for the creation of cyber security educational material. The paper will also argue in favour of the use e-learning as a delivery mechanism for such content. As such, the guidelines will be proposed in the context of a Moodle 2.0 e-learning environment.

Information Security Awareness; Brain Compatible Learning ; Cyber Security; Information Security

I. INTRODUCTION

Most current approaches towards information security education fail to pay sufficient attention to pedagogical theory [1]. The creation, distribution and manipulation of information is integrated throughout all aspects of modern society. Users; members of the general public, businesses and other facilities; require access to information in order to successfully conduct various daily transactions, both in a personal and/or professional capacity. Information is a valuable resource and any loss, unauthorized alteration, or corruption of it can have serious implications for all the users who rely on the information. It is therefore imperative that the protection of the confidentiality, integrity and availability of information as a vital resource is given appropriate recognition and attention *before* a problem can occur.

Security is a multi-faceted problem, the comprehensive solution to which will normally encompass physical, procedural and logical forms of protection [2]. From an organizational perspective, many international standards, such as ISO/IEC 27002 deal with the protection of this resource. For people in their personal capacity, there are currently no specific information security standards available. However, it could be argued that the protection of information in either a personal or organizational context would have to be based on the same general principles.

Standards such as ISO/IEC 27002 suggest the use of various information security controls as countermeasures to avoid, counteract or minimize security risks faced by informational resources. These suggested controls are categorically defined as physical, technical or operational in nature. Operational controls include administrative, managerial, and procedural and various other types that relate to the role(s) humans play in the information security process.

Physical controls provide a physical layer of protection. For example, a lock on a computer or server room's door could be described as a physical control. Technical controls would consist of technological countermeasures. For example, requiring users to authenticate themselves by logging into a system before being allowed to access the resources could be described as a technological control. Operational controls are controls which address the role(s) of humans. An example of such a control could thus be a policy statement requiring users to lock their office door when not in the office, or to logout of the system when they leave their computers. Both the physical and technical controls would therefore depend on the humans involved in the processes for their effectiveness. People involved in the information security process thus play a vital role in the effectiveness of the information security process and must therefore be **educated** about their necessary role(s) and responsibilities.

One of the most important pillars on which any serious effort towards information and cyber security is based, is the level of awareness (knowledge) that those responsible for managing the effort have. Therefore the issue of proper awareness, training and education of the involved people is of paramount importance. Most standards recommend that it is the lack of knowledge; regarding the roles people play, the responsibilities people and threats that exist in relation to the

information; which must be addressed via information security awareness, education and training programs. However, these programs are often constructed by security specialists who are not necessarily educationalists and might thus fail to adequately educate the users involved.

This paper will focus on pre-emptive education as a way to control information security risk. Furnell, Gennatou and Dowland [2] state that in businesses the inclusion of security-related issues is an integral part of any organizational training strategy and mechanisms to promote awareness during day-to-day activities. This extends to the members of the general public. The education of "average", daily users; members of the public; about information security and its related issues is vital to protect the information used in their daily lives. The educational material should be based on a set of sound information security principles. This paper will critically evaluate a general information security education program aimed at end users at the Nelson Mandela Metropolitan University (NMMU). It will then recommend guidelines for a more pedagogically appropriate presentation method of the subject-matter based on brain compatible learning theory principle and techniques. The paper takes the form of a case-study. The next section will examine current approaches towards information security education in order to identify problems in these approaches. This will be followed by a brief overview of brain compatible learning. The paper will then present a case study demonstrating how brain compatible learning principles can be incorporated into an existing information security educational program.

II. Current Approaches towards Information Security Education

Alnatheer and Nelson [3] state that security training and awareness programs are fundamental components of effective information security. Although this statement was made in the context of an organizational environment, it's extendable to the general public. The purpose of all these programs is to educate a certain target user group regarding information security. The scope of the subject's content matter and the extent to which the program aims to educate the user is vastly dependent on the "level" of the educational program. Security educational programs usually aim at one of three "levels" of education, namely; security awareness, training, or education [4].

The complete and comprehensive education of the users in cyber security involves a continuum of three levels of education. Each level advances the knowledge gained from the previous level and ultimately a comprehensive knowledge base of understanding is developed for and taught to the user, answering questions such as "what", "how" and "why" [4, 5]. These levels correspond to different types of learning, mostly delineated by differences in the degree of comprehension and detail, both of which increase as we move from awareness towards education.

The awareness level consists of a set of awareness activities. As explained by Katsikas[5] and the NIST Special Publication 800-16[4], awareness level activities are not a form of informal informative training, they are simply activities which aim at attracting the attention of individuals to the subject. The targeted audiences (the general users i.e. the members of the public) are mostly passive recipients of information and the knowledge gained through them tends to be short-term, immediate and specific, unless the activity is repeatedly exercised. This level answers the "what" question. Examples of possible presentation formats are posters, flyers, video tapes and promotional trinkets branded by motivational slogans. For the content of the information security awareness level NIST; the National Institute for Standards and Technology offers a full array of customizable awareness materials and resources for utilization. NIST [4, p. 15] states that "Effective IT security awareness presentations must be designed with the recognition that people tend to practice a disassociation (tuning-out) process called acclimation". As a result of this in order to prevent the target learners(members of the general public) from ignoring the awareness campaigns materials, the presentations must be on-going, creative, and motivational, with the objective of focusing the learner's attention so that the learning will be incorporated into conscious decision-making. The purpose of this level is to enable the user to recognise cyber security threats. The training level is more formalised and aims to develop the user's knowledge and skills, so as to allow them to take appropriate action against the identified threats.

The training level of the learning continuum aims at building knowledge, thereby producing relevant and needed security skills [4,5]. This level involves the development of high-level concepts and skills and therefore its execution and completion period is usually more extended than that of the awareness level [4,5]. The knowledge taught throughout the training process teaches the user how to solving problems by using the skills which are developed by the training process. This level answers the question of "how". Unfortunately an innate flaw of training as discussed by Katsikas [5] is that because training activities are directed towards exposing trainees to available knowledge and techniques for problem-solving, knowledge gained through them tends to be long term, but quickly becomes obsolete and therefore its impact time frame is only that of an intermediate timespan. Training must take into consideration that not all trainees require the same level of training. This is because the baseline security requirement for different individuals varies according to each user's personal requirements, experience and purpose for undergoing the training. "The level of training one receives in any particular training area, according to the individual's background and already acquired skills. This may be covered by assigning a degree of difficulty (or insight) to each course, ranging from beginning, through intermediate to advance" [5]. Examples of training formats are lectures, interactive demos, case studies and self-practice.

As explained by Katsikas and NIST [4,5] the education level of the learning process aims at creating expertise necessary for information systems security specialists and professionals. This level integrates all of the security skills, theory and knowledge taught by the previous levels into a single body of knowledge and it expands upon it to form a complete and comprehensive understanding of the entire subject [4,5]. A less technically intensive format than explained

by NIST for professionals could be adapted for general public users. The objective of the educational level is to develop the users' understanding of what has been taught on the previous levels, it answers the "why" question. The impact timeframe of this level is long-term. Examples of formats which the educational levels presentations can be are seminars, discussions, research and reading.

A. Problems with current security education

Many existing information and cyber security education courses are not completely successful. This is a result of several issues surrounding the courses, their presentation formats, and their content. One of the first problems is that people simply are not aware about their own need to take such an educational course. If people are not aware of the reason for the educational course, they will not make an effort to understand or learn from the course. The second problem relates to the subject matter itself, although the technical controls themselves exist, the operational procedures related to these controls often do not exist and therefore educational material relating to them is either non-existent or too vague to matter. This problem is extended by the third problem, which is that even if there are operational guidelines available for utilization in a business environment, there are normally no operational guidelines in existence for the general public, the source of the businesses work force. The other problems are mainly people (user) oriented or related.

One of the major problems is that people are not motivated to learn about information security. In an organizational context, Valentine [6] supports this by explaining that many employees, specifically those that do not interact with sensitive information, do not care about information security or social engineering. This is true in the public domain as well. The next problem is that people tend to forget what they have learnt in the educational course and therefore it results in the attendance and completion of the course being useless as the person has not truly learnt anything. Why people forget what they have learnt shall now be expanded upon.

There are numerous reasons for people forgetting what they have learnt, however these reasons may be categorized to relate to the course material, the course presentation or the learners themselves. The first reason could be that because the course material is set by security experts who do not necessarily have educational experience, and as such the material may be presented in a manner which is difficult to learn .This point is supported by research from Puhakainen [1]. Puhakainen states that most current information security educational approaches lack a sound theoretical basis. Goucher [7] states that security awareness training for the non-IT staff is often best delivered by security specialists who are not IT focused themselves. Conversely material set by educators may not be comprehensive enough to cover the subject; and although it would follow pedagogical theory no useful knowledge would be gained by the learner. Another problem could be that; as highlighted by Schultz [8]; the security training and awareness effort could simply be subpar; appearing as a figurative compliance to a standard of providing education and training; instead of being of a suitable standard to provide practical and useful education about needed skills and knowledge which could aid in an attendees. Schultz explained this in a business context, but the concept can be extended to carry over into the public domain to say that these courses should teach information and cyber security knowledge and skills need in member of the public's daily life[8].

The next reason is people may forget what they have learnt; this relates back to the actual development if the course material. Many training and education programmes do not consider the learners entry knowledge and skills, this is explained by Schultz and NIST. NIST specifically states that "material developers and trainers should consider the likely education and experience of their target audience and adjust their presentation approach and content accordingly." However many materials developers fail to take this into account and therefore many traditional employee security awareness programs utilize a very "one-size-fits-all" approach [6,8]. This ubiquitous approach is quickly becoming obsolete [6] and therefore leaves many attendees puzzled and many others bored, disappointed, and even hostile because they have learned nothing new [8].

The next possible reason is that course content is not interesting and therefore the learners could simply fail to pay attention to the lessons and therefore fail to benefit from what is being taught.

Finally, regardless of the interest level in the course content, people may simply fail to remember what they have learnt because the course material may not have been presented in a memorable manner and therefore the course content may fail to make an impression with the learner. This reason can be supported by the fact that different people have different learning styles. This argument is supported by NIST which states "Individuals learn in several ways but each person, as part of their 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"[4]. NIST then elaborates on the types of learning styles people may prefer and how they may be applied in a course. The learning styles mentioned are visual, auditory and kinaesthetic-tactile in nature [4].

In order to maximize the impact of such educational programs it is essential to not only focus on the content of these programs, like many security specialists do, but to also focus on the delivery of the content. One promising pedagogical approach which could improve the retention of knowledge by the "learners" in an information security program is *brain-compatible learning*. The next section will briefly introduce this pedagogical approach.

III. WHAT IS BRAIN-COMPATIBLE LEARNING?

A. How the Brain Learns

When presented with the concept of the learning process, one automatically associates the process with the mind and the brain. Therefore a brief explanation about the brain is necessary, but an in-depth discussion is beyond the scope of this paper.

The brain is divided into two linked hemispheres. The left hemisphere of the brain handles activities such as language processing, while the right often deals with music and spatial awareness. Whatever we are doing, however, both sides of the brain are nearly always involved in some way, and information flows back and forth in a continual dialogue [9]. According to Caine and Caine [10] the physical structure of the brain changes as the result of experience, this is called "brain plasticity". This means that as the brain is stimulated the brain will grow physiologically. According to Scoffham "learning and cognition appear to consist in establishing patterns between brain cells" [9], Scoffham explains this concept further. Modern scientists believe that the cortex is organized into several hundred million neural networks or modules [9]. These modules extend vertically through the cortex in small columns, which are then linked up into more complex structures. New experiences physically change the brain by causing neurons, the brain cells principally involved in cognition, to sprout new branches, or dendrites, and thus increase communication among neurons across microscopic gaps called synapses. The synaptic leap of an electrical impulse between the axon of one neuron and the dendrite of another is the physical basis of learning and memory. Once the cellular pathway has "fired" repeatedly a chemical change occurs which makes it more likely to trigger in future and become increasingly efficient. This is called 'Hebbian learning', and is the physical goal of brain compatible learning techniques.

B. Defining Brain-Compatible Learning

Leslie Hart defined the term "brain-compatible" as the education designed to match "settings and instruction to the nature of the brain, rather than trying to force (the brain) to comply with arrangements established with virtually no concern for what this organ is or how it works best."[11] Jensen defined brain-compatible (brain-based) education as the "engagement of strategies based on principles derived from an understanding of the brain." Therefore we can safely devise that brain-compatible learning is learning based on brain-compatible education principles, methods and techniques which endeavor to teach subject matter in a manner and format which is naturally complimentary to the brains physical and psychological processing functions.

In the context of a classroom environment Rogers and Renard [12] explain that brain-compatible, research-supported teaching techniques allow students to move around the classroom, address multiple modes of learning, acknowledge outlets for creative presentation of learning, provide enough contrast to preclude boredom, and contribute to a motivating context. It also allows teachers to employ summarization; provide anticipatory and closure strategies; and ensure a tight alignment among curriculum, instruction, and assessment. This means that brain-based education uses evidence from all disciplines to enhance the brains of students [13].

Brain-compatible learning has several principles as a general theoretical foundation [10]. The principles are simple and neurologically sound. Applied to education the brain compatible principles guide educators in the defining and selecting of appropriate educational programs and methodologies [10]. Some of these principles will now be discussed.

One of the most important principles of brain-compatible learning is that "Emotion is the gatekeeper to learning"[14]. Everything learners "learn is influenced and organized by emotions and mindsets involving expectancy, personal biases and prejudices, self-esteem and the need for social interaction"[10]. A learner's emotional state is resultant of their body's chemical messaging system. This state affects their attention and ability to focus and therefore it affects their ability to learn. Ornstein and Sobel, Lackoff, McGuinness and Pribram and Halgren et al. (cited by [10]) state that emotion and cognition cannot be separated. Implication of this principle in relation to cyber security education is therefore that the course content should be implemented and presented in a manner that provides a supportive environment, which is no-threatening to the learner and encourages cooperative approaches to learning.

Another brain compatible principle is that the brain stores most effectively what is meaningful from the learner's perspective [14]. Caine and Caine [10] explain this as "patterning". During the learning process, the brain attempts to distinguish and understand patterns which appear in what is being learnt or experienced. The brain naturally integrates and assimilates information, which may initially seem random and disconnected, provided that the initially isolated information is related to what makes sense to a particular student. Implications for the education of the learners are that the subjected material should be presented in a format which encourages problem solving and critical thinking.

Other brain-compatible education principles do exist, but a complete in-depth study and analysis of the brain-compatible principles is beyond the scope of this paper, however specific principles will be dealt with in more depth as part of the case study.

IV. METHODOLOGY

The remainder of this paper will take the form of a case study, as described by Cresswell [15] and follows the structure suggested by Creswell. This structure is as follows:

- Entry vignette
- Introduction
- Description of the case and its context
- Development of issues
- Detail about the selected issues
- Assertions
- Closing vignette

V. INTRODUCING SEAT

A cyber security training and education programme which is presented in a memorable format and complies with sound

pedagogical theory is needed. The aim of this section is to perform a critical evaluation of the Security Education and Training (SEAT) programme at the Nelson Mandela Metropolitan University (NMMU). It will then aim to propose a set of brain compatible learning guidelines for the creation of cyber security educational material which can be used to update and improve the current SEAT programme.

A. Introduction

In the first section of this paper it was established that information is important, and members of the general public need to be taught how to protect it. It was then further discussed and a need for cyber security training and education programme which is presented in a memorable format and complies with sound pedagogical theory; namely brain-compatible education theory; was established. An existing information security programme is the SEAT training and Education programme at Nelson Mandela Metropolitan University (NMMU), however this programme is not presented in a brain-compatible educational manner. The programme must be evaluated and brain-compatible guidelines should be proposed, so that the SEAT's education material may be edited and updated to be presented in a brain-compatible manner so as to increase the success rate of the courses students.

VI. THE SEAT DESCRIPTION

A. The Overview

SEAT is a security education and training course at the Nelson Mandela Metropolitan University (NMMU). Its objectives are as follows:

1. To improve the awareness of the need to protect system resources and an organizations end users.
2. To develop the skills and knowledge of computer users so they may perform their computer activities more securely.
3. To allow online access to a rich source of security related best practices.
4. To help end users understand why security is part of their responsibilities, and how they impact the security of the organizations they work for.

The course material covers nine modules; each of which covers a specific topic. Each module has a corresponding quiz to test the learners understanding of the covered material; to progress through the course each chapters quiz must have been successfully completed and passed to allow progression to the next chapter. Once all the modules and quizzes have been completed, there is a final exam, covering all the material covered. The module topics are as follows:

1. Security in General – an introductory explanation of security and security related terminology
2. Information Security – an explanation of the importance of security information and provides methods to secure said information
3. Password Security - provides the learner with best practices for choosing secure passwords
4. Virus Awareness - provides information on various types of viruses, virus detection and prevention
5. Data Storage and Backup - provides best practices about how to secure data during storage
6. Computer Ethics – outlines appropriate behaviors for computer users
7. Office Discipline - outlines how system users should behave in the office environment
8. Hardware Security - addresses the protection of hardware devices
9. Social Engineering - covers Social Engineering and the techniques to combat such attacks

Currently each module lesson is presented in a single flash file presentation. Each topic's presentation module covers several related sub-topics. The module's flash slides content presentation consists of text and representative images. The text is presented mainly in bullet points and brief explanations, while the images are embedded throughout the presentation. The quizzes consist of multiple choice questions.

This course is currently running, however it has been noted that this courses material and presentation method is outdated and SEAT needs to be redeveloped. It is therefore a sensible solution to update the presentations to be presented in a more brain-compatible manner, so as to improve the success rate of learners who take the course. The section will outline the courses specific issues which will need to be improved, as part of the courses redevelopment.

VII. DEVELOPMENT OF ISSUES

The SEAT course has three categories of issues which must be rectified during the courses re-development. This section will briefly outline them all, but it will focus on the category which relates to the presentation of the course content, as the other two categories fall beyond the scope of this paper.

The first category of issues relates to the actual deployment and maintenance of the SEAT programme. The original SEAT program is a program which was developed in-house at the university a few years ago. Over time certain issues have been identified relating to the running and updating of the program. The first issue relating to its deployment and continued functioning is that the program has a problematic tendency to "crash" or cease functioning correctly. The other issues all relate to the maintenance and continual updating of the program and its content. The first maintenance issue is that the programme is generally difficult to maintain. The updating of the content is time-consuming and unstructured, the modification of code is impossible. The following issues detail why the first issue exists. One of the major issues is that the original developers of the SEAT platform are no longer in the employ of the university and they are therefore not available to

perform the required updates and modifications. The programme development and maintenance instructions were poorly documented and no other developers have been able to sufficiently understand what was documented enough to risk modifying what was in existence. The modification itself has been deemed impossible as the SEAT program was developed using an older version of the development tools used by the university and the code is not compatible with the current toolsets.

The second category of issues relates to the actual content which is covered in the SEAT course. The main content issue is that the course's material is outdated. Although the scope is large and covers many aspects of information security, the course fails to cover many of the newer security threats that have come in to existence in that last decade and conversely still covers many security threats which have been mitigated by their progression into an obsolete existence. An example of the continued education about obsolete threats is the continued focus on floppy-disk media and an example of the threats which are not covered is the failure to highlight the threats from social networks, portable storage media such as flash drives, and the new portable technologies such as iPods and portable media players.

The third category is the one that this paper is mainly focusing on; the presentation of the course. According to a brain-compatible education principle educational material should engage multiple sensory channels in order to have maximum impact for the rehearsal of new learning concepts. SEAT only has one mode of presentation, in the format of the modular flash files; consisting of text and image contents; which only has a visual impact and does not cater for all learners ideal learning style. The SEAT programme currently provides no feedback to the learner aside from mark earned at the end of the quiz and a display of the questions which were incorrectly answered. This should be rectified to comply with the principle which states that feedback is vital. The material being presented seldomly utilizes the learner's positive emotions to aid learning and recall. The content is presented in a factual manner, to which the student may not necessarily relate. A brain-compatible principle which is related to this issue states that all new material should be relatable back to old material which may have meaning to the learner. The material is only covered in two tasks. First the topic is taught using the single flash file presentation and then a short quiz is administered. This is an issue because there is a principle which suggests that material should be repetitively reviewed to solidify recall and recognition of the taught material.

The issues identified relate to seven selected brain-compatible education principles. These issues will be elaborated on in the next section.

VIII. Detail about the selected issues

In this section the aforementioned deployment and maintenance, content and presentation issues will be discussed.

The first deployment and maintenance issue of the in-house deployment has been mitigated by the transference of the SEAT course material to Moodle. Moodle is an open and modular system of educational content distribution and user management [16]. It is a cost effective solution since the software Moodle is available from General Public License (GNU). All instability issues from the previous SEAT course with relation to stable deployment have been subsequently resolved. This transference to the Moodle platform also prevents the issues of the unavailable developers, the outdated and unsupported development tools and the lack of system development documentation since Moodle is an open-source fully documented project and all development issues are tracked by Moodle Tracker.

Valentine states "the traditional employee security awareness model provides a static solution for a fluid problem" [6]. He explains that information security is a constantly evolving field because of the continuous creation of new threats, techniques, countermeasures and philosophies and therefore any security awareness course can only provide an adequate explanation of information security as it currently exists if the curriculum is completely up to date. The course material covers old security risks and threats; such as floppy disks, and does not cover new security threats; such as social network threats, newer technology threats such as iPods, iPads, kindles and portable media players etc. As previously stated SEAT's course material needs to be updated, however this is beyond the scope of this paper.

The other issues are all related to the presentation of the course and will be solved by the redevelopment of the course and the application of brain-compatible education principles.

The first brain-compatible education principle states that the rehearsal of new learning concepts should involve a combination of multiple sensory channels. This principle is supported Scoffham [9] who states "rich experiences can promote brain growth while sensory deprivation can inhibit it". As a whole this principle promotes development of educational material which caters different learning styles. NIST [4] encourages instructors to be aware of different learning style differences and to utilize a variety of teaching approaches to cater for all the styles. Laurie Materna in her book; Jump start the adult learner: how to engage and motivate adults using Brain-compatible Strategies; states that the use of many combined teaching strategies that promote learning across all learning styles is a good educational solution [17]. Materna states that "promoting activities that activate seeing, hearing and feeling facilitates much more productive, efficient and long lasting learning" [17]. The implications of this on the SEAT course are that the course should be expanded to include multiple media options for the coverage of the educational material. Auditory learners understand educational material better after listening to the material rather than after reading the material. To cater for the auditory learning style the following examples of media expansions should be the included into the course:

- auditory streams of the lessons
- narrated flash slide presentations
- forum for discussions and sharing of media and documents)

- wikis (collaboratively-built pages useful for group work and other negotiations) will be included

Visual learners learn by reading and examining pictures, graphics, graphs and demonstration media. Scoffham states that "visual presentation techniques serve to extend pupil's skills beyond the rather narrow confines of linguistic and logical-mathematical thought and to explore links and connections that might not otherwise be apparent"[9]. Additions to the SEAT course which could cater for the visual learners to a larger extent are the following:

- existing flash presentations
- videos of the classes and scenario enactments
- the presentations themselves should include many graphics, charts, diagrams

Finally the kinesthetic-tactile learners prefer to learn by performing physical activities, such as doing hands-on activities and performing practice activities. The course modifications which could make a difference for the kinesthetic-tactile learners are the following:

- Interactive lesson exercises
- Task simulations
- Games which emphasize the lessons concepts learnt

All of these activities will be combined and sequentially grouped to guide the learners through the course.

The second brain-compatible education principle which will be applied to the SEAT course is the principle which states that the presentation of the material should utilize the learner's positive emotions to aid learning and recall. This principle is important because "the brain does not naturally separate emotions from cognition, either anatomically or perceptually"[9,10,18]. Learning is dependent on a feeling of security and a lack of threats [13].Fostering positive feelings in the learning context of the course will enable students to value the courses activities enough to want to learn and to achieve. Rogers and Rebard explain that when a person's psychological needs are met, they are more likely to perform well in order to experience positive emotions and therefore we can deduce that by maintaining a constant cycle of positive emotions through satisfaction with work completed and interest and happiness with work being done, we can motivate learners to consistently learn material well enough to later easily recognize or recall it [12]. "Intellectual learning and emotional involvement are linked together in the fabric of the brain [19]. The implications of this principle on the course are the following:

- The material will be presented in a manner which relates it to the learners to issues or circumstances that they can relate to personally. This is because "learning occurs only when what is being presented is meaningful enough to the student that he or she decides to actively engage in the learning experience "[10]. Being meaningful to the learner often means that the activity satisfies specific human emotions.
- The previously mentioned interactive lesson exercises, task simulations and games also serve to engage the learner's emotions.

  Feedback will be provided for each quiz, activity and interaction with the material once redeveloped.

The third brain-compatible principle is to relate all new material back to old material rebuild new knowledge on old knowledge. This principle promotes assimilation; the process whereby an individual incorporates new experiences into an existing behaviour pattern [4]. This is because learning only occurs when what is being presented is meaningful enough to the student that he or she decides to actively engage in the learning experience [9,10,12]The implications of this on the course are as follows:

- The presentations will include enquiry questions."Enquiry questions draw pupils into a problem so that they relate new learning to their previous knowledge and understanding. Without this link, the patterns between brain cells are not properly established"[9].
- The previously mentioned slides, videos, task simulations can be related to real-life problems. Scoffham states that thinking about real-life problems harnesses the brain's natural capacities [9].
- Activities which can be related to the module will be embedded in the lessons. An example would be the task simulations

The sequential grouping of all the activities in Moodle allows each activity to be built on the outcomes of previous ones, this promotes this principle.

The fourth brain-compatible principle is to repetitively review material to solidify recall and recognition. Jensen explains that repeating what we have learnt helps the learner to feel emotionally sure that what has been learnt is true [20]. Subsequently it is good practice to encourage learners to reinforce what they have learnt by presenting the material in multiple formats as discussed in relation to the first principle.

Moodle supports many types of built-in activities for example forums, glossaries, wikis, assignments, quizzes and choices (polls). Moodle also allows activities which on aren't supported by Moodle itself to be integrated into the lessons via plug-ins. This flexible characteristic of Moodle allows the educators (security course developers) the opportunity to provide learners multiple options for revision material.

The fifth brain-compatible principle is to allow learners to progress through the course at their own pace. People learn at different rates, so this principle is highly appropriate for learners to be able to have control of their training and adjust it to their own personal needs. Allowing learners to progress at their own pace provides them with a larger chance at successfully completing the course and allows learners to acquire the desired training in information security in a flexible manner. In compliance with this principle the following changes will be made to the SEAT course:

- Students will chart their progress, via the use of mark sheets and use logs. Renard and Rogers explain the use of learning logs use learning logs allows learners to reflect upon what they are capable of after completing the lesson in contrast to what they were capable of before the lesson [12]. It "allows them to see their successes"[16]. In Moodle the user log reports show detailed logs of every action taken by a person in Moodle, as well as graphs showing overall activity statistics.

There are many other brain- compatible education principles which could be applied, but these five are the most appropriate for the e-learning; Moodle; environment.

IX. Assertions

Firstly, the authors wish to assert that, based on the performed evaluation, **the NMMU SEAT course can be improved**. Both the presentation and the content aspects of the course require updating. This paper examined the presentation solutions, the content issues fall beyond the scope of the current paper but will be examined in future work.

The first categories of deployment and maintenance issues have already been solved successful by the transference of the course material to Moodle 2.0. Since Moodle was designed to be used to support a number of other pedagogical and andragogical approaches and its modularity, flexibility, security and free availability are advantageous for the courses redevelopment, Moodle has proven to be an appropriate choice for the new SEATs deployment. Since Moodle is an open-source platform, this is a cost effective solution. **E-learning courses aimed at cyber security education should preferably be developed on widely used and supported e-learning frameworks and not on "in-house" platforms**.

The courses content needs to be constantly updated. Information and cyber security are both constantly evolving fields. As new threats are developed, so must combative solutions come into existence. As these solutions are developed they should be taught to the learners, in this case, the general public. **The content currently presented in the SEAT course is out of date.** However the redevelopment of this content is beyond the scope of this paper.

Brain-compatible techniques can be used to improve the presentation of both the existing and the future course material. It has been established that many existing security education programmes fail and that this is possibly because they do not have a sound pedagogical basis. Therefore information and cyber security researchers should consider brain-compatible education as a possible pedagogical approach to act as a solution for the problem.

Brain-compatible techniques require a significant investment in the development of content. Since content need to be presented in multiple formats making use of, for example, multimedia, the development of content could also require skills that a typical security expert might lack.

X. Conclusion

The improvements to the SEAT course have not as of yet been tested empirically; however such a "field test" will be part of the next stage of the current research. Having evaluated the existing SEAT course, the brain-compatible pedagogy and the possibilities which arise from the combining of the two facets, it can be stated that the cyber security educators who develop security awareness, training and education courses can and should learn from educationalists about the appropriate pedagogical approaches exist and they should incorporate them into their courses.

XI. Bibliography

[1] P. Puhakainen, "A design theory for information security awareness," University of Oulu, 2006.

[2] S. Furnell, M. Gennatou, and P. Dowland, "Promoting security awareness and training within small organisations," *1st Australian Information Security Management Workshop University of Deakin Australia*, 2000.

[3] M. Alnatheer and K. Nelson, "QUT Digital Repository :," *7th Australian Information Security Management Conference*, 2009, pp. 1-3.

[4] J.D. Tressler, J.B. Ippolito, and P.-based Model, "Information Technology Security Training Requirements: A Role- and Performance-Based Model," *Nist Special Publication*, 1998, pp. 15-21.

[5] S.K. Katsikas, "Health care management and information systems security : awareness , training or education ?," *International Journal of Medical Informatics*, vol. 60, 2000, pp. 129 - 135.

[6] J. Valentine, "Enhancing the employee security awareness model," *Computer Fraud Security*, vol. 2006, 2006, pp. 17-19.

[7] W. Goucher, "The Face of Security Getting the most from training sessions: the art of raising security awareness without curing insomnia1," *Computer Fraud & Security*, vol. 2008, 2008, p. 15.

[8] E. Schultz, "Security training and awareness—fitting a square peg in a round hole," *Computers Security*, vol. 23, 2004, pp. 1-2.

[9] S. Scoffham, "Geography, learning and the brain: An example of literature based research," *Researching Primary Geography*, 2004, p. 120–28.

[10] R.N. Caine and G. Caine, *Making Connections: Teaching and the Human Brain.*, Association for Supervision and Curriculum Development, 1991.

[11] L.A. Hart, *Human brain & human learning*, Books for Educators, 1998.

[12] S. Rogers and L. Renard, "Relationship Driven Teaching," *Educational Leadership*, vol. 57, 1999, pp. 34-37.

[13] E.P. Jensen, *A fresh look at brain-based education*, 2008.

[14] J. McGeehan, "Brain-Compatible Learning.," *Green Teacher*, vol. 64, 2001, pp. 7-13.

[15] J.W. Creswell, *Qualitative inquiry and research design*, Sage Publications, 2007.

[16] G. Futa and B. Gocłowska, "Analysis of functionality of distance learning platform moodle," *Portal*, vol. 3, 2005, pp. 331-338.

[17] L. Materna, *Jump start the adult learner: how to engage and motivate adults using Brain-compatible Strategies*, California: Corwin Press, 2007.

[18] A.R. Damasio, *Descartes' Error: Emotion, Reason, and the Human Brain*, Putnam, 1994.

[19] R. Carter, *Mapping the Mind*, University of California Press, 2000.

[20] E. Jensen, *Brain Based Learning and Teaching*, Turning Point Publishers, 1995.