An Integrative Approach to Information Security Education: A South African Perspective

L. Futcher, C. Schroder and R. von Solms

Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
e-mail:{Lynn.Futcher, Cheryl.Schroder, Rossouw.vonSolms}@nmmu.ac.za

Abstract

The importance of information security cannot be denied. It has increasingly become an integral part of our everyday lives. In line with some of the key issues relating to the construction of a South African education and training system for the 21st century, this paper argues that information security is both 'a social and economic need' and 'an intellectual and professional challenge' and should therefore be regarded as a critical cross-field outcome. This could help narrow the evident 'information security gap' that currently exists in undergraduate IT/IS/CS curricula at South African universities.

Keywords

Outcome-Based Education (OBE), Critical Cross-Field Outcomes (CCFOs), Information Security Education, IT/IS/CS Curricula

1. Introduction

'Globalisation and modernisation are creating an increasingly diverse and interconnected world. To make sense of and function well in this world, individuals need to master changing technologies and to deal with large amounts of available information. In addition, they also face collective challenges as societies - such as balancing economic growth with environmental sustainability, and prosperity with social equity. In these contexts, the competencies that individuals need to meet their goals have become more complex, requiring more than the mastery of certain narrowly defined skills' (OECD, 2005).

Information security is important in any organization. Firstly, from a social perspective, people are increasingly using technology to communicate, collaborate and interact with one another using social networking platforms like Facebook, MySpace and Orkut. These online communities involve grouping people together to share common interests regardless of their physical location. The internet provides everyone across the globe with access to various online tools and applications, infinite information sources and social networking sites. Unfortunately, with these social benefits come certain dangers including online predators, personal data theft and viruses.

Secondly, from an economic point of view, information insecurity is costing organizations billions of dollars each year. This lack of attention being paid to security is being paid for in theft and in productivity losses (Schneier, 2008). Higher

education is required to contribute to economic development and to prepare learners for employment. It is therefore becoming increasingly important that anyone entering the professional workplace needs to be able to demonstrate an understanding of the underlying principles of information security and their role and responsibility in this regard. We therefore argue that information security education could play a key role in overcoming this economic dilemma.

Thirdly, as an intellectual and professional challenge, Manjak (2006) states that 'Information security must be generally recognized and accepted as a distinct value within the institutional culture that informs and influences employee behaviour'. From this it is evident that information security has become an integral part of our everyday lives and that organisations recognise the influence which it has on the behaviour of employees.

The challenge for educational institutions is to equip learners with the knowledge, values, skills and attitudes necessary to ensure that they are able to participate responsibly within their communities and contribute towards the economic development of their societies.The Department of Education (DoE) is responsible for regulating education in South Africa. The mission of the DoE includes aspects relating to 'ensuring the success of active learning through outcome-based education, creating a vibrant further education and training system to equip youth and adults to meet the social and economic needs of the 21st century and building a rational, seamless higher education system that grasps the intellectual and professional challenges facing South Africans in the 21st century' (Department of Education, n.d.).

This paper briefly discusses outcome-based education (OBE) with a specific focus on the broad learning competencies, commonly referred to as critical cross-field outcomes (CCFOs). This is followed by a brief overview of information security in the existing IT/IS/CS curricula in five South African universities. Finally it proposes that information security be regarded as a critical cross-field outcome to be addressed throughout the curriculum.

2. Outcome-Based Education

In 1997, the ministry of education in South Africa launched an outcome-based system of education, referred to as Curriculum 2005. The primary notion behind the development and maintenance of this OBE system was to redress the educational imbalances of the past by creating an opportunity for all South Africans to become lifelong learners.

OBE requires that learning programmes be described in terms of measurable exit outcomes which learners are required to attain. These outcomes are described as the end product of the learning process, i.e. they are the desired end results expected of learners in order to demonstrate what they understand. These results are measurable and may be the evidence of formal or informal learning.

In OBE, curriculum developers work backwards from agreed desired outcomes within a particular context. In the National Standards Bodies (NSB) regulations, a qualification is described as representing a planned combination of both specific and CCFOs that promote lifelong learning (South African Qualifications Authority, 2000). The outcomes specified for a particular qualification are typically derived from:

- The specific knowledge, skills and attitudes needed for entry into the workplace (i.e. professional expectations);
- The general knowledge, skills and attitudes needed for entry into the workplace (i.e. broad, generic, underpinning competencies);
- Current and future trends in the world of work (eg. the need for innovation and flexibility in the work place)

It is therefore important that curriculum developers adapt their curricula according to the current and predicted trends, whilst take into account the specific needs of industry and the broad competencies required to fully prepare learners for entry into the workplace. The following section describes these broad competencies in more detail.

3. Critical Cross-Field Outcomes

Today's societies place challenging demands on individuals who are confronted with many complexities in their day-to-day lives. It has therefore become necessary to identify broad underpinning competencies that prepare learners for these challenges, whilst at the same time meeting the overarching goals of education and life-long learning. In South Africa, these competencies are referred to as critical cross-field outcomes (CCFOs).

The CCFOs adopted by SAQA are an additional mechanism through which consistency is achieved in the National Qualifications Framework (NQF). These CCFOs are deemed critical for the development of the capacity for life-long learning, regardless of the specific area or content of learning. Proposers of qualifications must ensure that all CCFOs have been addressed appropriately at the level concerned within the qualifications being proposed (South African Qualifications Authority, 2000). Based on these CCFOs, all learners must develop the ability to:

- identify and solve problems in which responses show that responsible decisions, using critical and creative thinking, have been made;
- work effectively with others as a member of a team, group, organization or community;
- organise and manage themselves and their activities responsibly and effectively;
- collect, analyse, organize and critically evaluate information;
- communicate effectively using visual, mathematical and/or language skills in the modes of oral and/or written presentation;
- use science and technology effectively and critically, showing responsibility towards the environment and health of others; and

- demonstrate an understanding of the world as a set of related systems by recognizing that problem-solving contexts do not exist in isolation (South African Qualifications Authority, 2000).

In addition, the following skills are considered important in the personal development of learners:

- reflecting on and exploring a variety of strategies to learn more effectively;
- participating as responsible citizens in the life of local, national and global communities;
- being culturally and aesthetically sensitive across a range of social contexts;
- exploring education and career opportunities; and
- developing entrepreneurial opportunities (South African Qualifications Authority, 2000).

When a qualification is registered, there is a requirement for the CCFOs to be articulated and therefore cannot be ignored in developing learning programmes. However, there is no prescription in any of the SAQA regulations of how these outcomes are to be incorporated and developed. The incorporation of CCFOs into the learning programmes therefore provides an interesting challenge to educators.

4. Information Security in the IT/IS/CS Curriculum

Information Security is a broad area of study. According to Ross (1999) it may be described in terms of domains, functional areas and concepts. The various domains may be categorized according to physical security, operational security, personnel security, systems security and network security. However, since information security is strongly related to risk, the functional areas need to address specific risk actions including risk avoidance, deterrence, prevention, detection and recovery. The concepts referred to by Ross include the high-level goals of security including confidentiality, integrity, authentication, access control, non-repudiation, availability and privacy.

A question regarding the extent to which Information Security is incorporated into the IT/IS/CS curricula at South African universities was raised by the authors. In order to answer this question, a brief survey was carried out. Responses were received from professors at five different universities. The first question posed was 'Do you offer a full a qualification dedicated to Information Security?'. None of the universities surveyed offer such a qualification. The second question asked was 'Do you offer undergraduate subjects or modules dedicated to Information Security?'. Sixty percent (3 out of 5) of the respondents indicated that they do offer undergraduate subjects dedicated to information security, one of which handled this as an elective. The subjects indicated as being provided at undergraduate level included Support Services, Information Systems Security and Controls and Computer Security. The final question posed was 'Do you offer postgraduate subjects or modules dedicated to Information Security?'. Eighty percent (4 out of 5) of the respondents indicated that they do offer postgraduate subjects dedicated to information security, although all respondents indicated that these are handled as

electives. These subjects included Information Security, Computer Security, Information Security in the WWW, Information Security Governance, Network Information Security and Information Security Risk Management.

These results suggest that education in information security has matured much more rapidly in postgraduate than in undergraduate programmes at South African Universities. Although the efforts at postgraduate level are promising, there is a concern that Information Security is not being adequately addressed in many undergraduate IT/IS/CS curricula. This may be contributed to the fact that these programmes are already under pressure to deliver a wide variety of subjects and modules that address the specific learning competencies required of IT/IS/CS professionals. Educators at South African universities need to investigate alternative means by which to address the gap thereby ensuring that Information Security receives the required attention in all learning programmes. A number of approaches exist.

Perrone, Aburdene and Meng (2005) describe three main approaches to instruction in security, namely single-course, track and thread. Although the single-course approach provides a considerable breadth of topics relating to security in one course in the curriculum (typically an elective), it does not provide much depth. In the track approach, a student may take a sequence of courses specializing in security and information assurance. Since this approach requires numerous expensive resources, it is not widely adopted. The thread approach, however, is a compromise one which bridges the gap between the single-course and track approaches by using security and privacy as a unifying theme across the core curricula. In this way it can effectively meet the security education needs of today's professionals using a minimum of resources (Perrone, Aburdene, & Meng, 2005).

Similarly, the ACM Special Interest Group for Information Technology Education (SIGITE) regards Information Assurance and Security (IAS) as a 'pervasive theme' that must be addressed during the entire learning experience (SIGITE, n.d.). Whereas a knowledge area represents a significant body of knowledge in a discipline, pervasive themes are topics that should permeate the IT curriculum since they cut across all knowledge areas. They also state that both learners and educators need to be consistently aware of how these pervasive themes need to be integrated into the curriculum (Dark, Ekstrom, & Lunt, 2006). The complete list of 'pervasive themes' comprising topics which are considered essential but not belonging to a single knowledge area includes:

- User advocacy;
- Information assurance and security;
- Ethics and professional responsibility;
- The ability to manage complexity through: abstraction and modeling, best practices, patterns, standards and the use of appropriate tools;
- A deep understanding of information and communication technologies and their associated tools;
- Adaptability;
- Life-long learning and professional development;

- Interpersonal skills.

In line with this idea, this paper proposes that information security be considered as a CCFO to be integrated across all learning programmes.

5. Information Security as a CCFO

Academic institutions too often view information security in isolation. Some view information security as solely a technical discipline. Although technical controls are helpful in mitigating some risks, it is important that technology alone should not be viewed as an information security solution. Technology is greatly impacted and influenced by the procedures and people resources within an organisation (ISACA, 2009). Each element of information system security has a link to the various information system components. People are integral to all information systems and people need procedures that provide the operating instructions for using an information system. Information security cannot be successfully dealt with without considering the people and procedural aspects and the important roles and responsibilities of all individuals in attaining the goals of information security. This poses the question of 'how can IT/IS/CS educators integrate information security into their learning programmes to ensure that learners realise their individual roles and responsibilities in meeting the goals of information security'. We argue that this can be achieved by considering information security as a core competency.

A competency is more than just knowledge and skills since it requires the ability to meet complex demands in a particular context (OECD, 2005). According to the OECD (2005), a competency must:

- contribute to valued outcomes for societies and individuals;
- help individuals meet important demands in a wide variety of contexts; and
- be important not just for specialists but for all individuals.

From this standpoint, we argue that since information is integral in virtually every aspect of a learners life, information security needs to be defined as a core competency to be addressed in all learning programmes. Information security may therefore be described as a broad, generic competency and as such, it may be worded as 'all learners must develop the ability to protect information by recognizing the major legal, ethical, privacy and security issues in information technology thereby ensuring its confidentiality, integrity and availability'.

According White and Nordstrom (1996), the integration of security across the curriculum should not come at the expense of other topics. Instead, security should enhance the learning of other topics. Information security may be categorised into many topics. However, not all such topics can be effectively addressed at undergraduate level. Being less technical in nature, the topics listed in Table 1 are typically those which could possibly be integrated into all learning programmes. These topics are based on the list of Information Security curriculum concepts proposed by Bogolea and Wijekumar (2004). Their comprehensive list was drawn up after compiling the results from various surveys, interviews, curriculum

comparisons and suggested government directives. The more technical topics like access control, cryptography and intrusion detection, however, are better integrated into specialized Information Security courses.

Topic	Detail
Information Security Fundamentals	Information Security challenges brought about by computers and the Internet Basic Information Security terminology Importance of protecting information assets Information Security realted issues, unauthorised or inappropriate access to information (eg. malicious hackers, cyberterrorism, physical security). Information Security concepts: confidentiality, integrity, availability, authentication, etc. Increasing Information Security awareness Threats, vulnerabilities, viruses and other malicious code Legislation and industry standards
Information Privacy	Why privacy is a major concern to individuals, businesses and government agencies Strategies for protecting privacy
Ethical and Legal Issues	Software piracy, code of ethics, privacy law, copyright
Information Security Policies	The role of information security policies Understanding Information Security policies, procedures and standards Acceptable Use Policies Compliance and enforcement
Password Security	Rules for good passwords, general password usage and management
E-mail Security	Handling e-mail and attachments from unknown sources Spam and e-mail etiquette
Internet Security	Using the internet securely (transmitting sensitive or confidential information over the internet) Using social networks responsibly
Data Management	Data storage, backup and recovery

Table 1: Information Security Topics

6. Conclusion

This paper is specifically concerned with satisfying the information security needs of the broader IT learner population as opposed to those learners showing an interest in becoming information security professionals. By explicitly defining information security as a CCFO it is anticipated that the 'information security gap' that currently exists in the undergraduate IT/IS/CS curricula at South African universities could be addressed. However, further research is required to investigate the extent to which the proposed information security topics can be seamlessly integrated into the various learning programmes. In addition, further research may also provide some insight as to why information security has matured more on the postgraduate level than on the undergraduate level.

7. References

Bogolea, B., & Wijekumar, K. (2004). Information Security Curriculum Creation: A Case Study. InfoSecCD Conference (pp. 59-65). Kennesaw: ACM.

Dark, M., Ekstrom, J., & Lunt, B. (2006). Integrating Information Assurance and Security into IT Education. Journal of Information Technology Education , 389-403.

Department of Education. (n.d.). Department of Education: Vision and Mission. Retrieved January 26, 2010, from Department of Education: http://www.education.gov.za/

ISACA. (2009). An Introduction to the Business Model for Information Security. Retrieved November 4, 2009, from http://www.isaca.org

Manjak, M. (2006, June 1). Social Engineering Your Employees to Information Security. Retrieved February 9, 2010, from SANS Institute - InfoSec Reading Room: http://www.sans.org/reading_room/whitepapers/engineering/social_engineering_your_employees_to_information_security_1686

Null, L. (2004, May). Integrating Security Across the Computer Science Curriculum. Retrieved February 9, 2010

OECD. (2005, May 27). The Definition and Selection of Key Competencies. Retrieved February 15, 2010, from http://www.oecd.org/dataoecd/47/61/35070367.pdf

Perrone, L. F., Aburdene, M., & Meng, X. (2005). Approaches to Undergraduate Instruction in Computer Security. Proceedings of the 2005 American Society for Engineering Education Annual Conference and Exposition. American Society for Engineering Education.

Ross, S. (1999). Computer Security: A Practical Definition. Retrieved November 30, 2009, from Albion: http://www.albion.com/security/intro-4.html

Schneier, B. (2008, August 10). The Problem is Information Insecurity. Retrieved February 9, 2010, from Bruce Schneier: http://www.schneier.com/essay-233.html

SIGITE. (n.d.). SIGITE Home Page. Retrieved January 24, 2010, from ACM SIGITE: http://www.sigite.org/

South African Qualifications Authority. (2000, May). The National Qualifications Framework and Curriculum Development. Retrieved January 26, 2010, from The South African Qualifications Framework: http://www.saqa.org.za/

White, G., & Nordstrom, G. (1996). Security Across the Curriculum: Using Computer Security to Teach Computer Science Principles. Retrieved March 30, 2010, from www-08.nist.gov/nissc/1996/papers/NISSC96/paper003/sec_cur.pdf