An Educators Perspective of Integrating Information Security into Undergraduate Computing Curricula

L.G. Gomana, L.A. Futcher and K. Thomson

Centre for Research in Information and Cyber Security, Nelson Mandela
Metropolitan University, Port Elizabeth, South Africa
e-mail: {s210031492, lynn.futcher, kerry-lynn.thomson}@nmmu.ac.za

Abstract

Information is an integral part of our everyday lives and organisations need to have their information and related systems protected from various threats that exist. Therefore, information security education is of vital importance to all computing learners. It is the duty of higher education institutions to ensure that information security is pervasively integrated into the undergraduate computing curriculum. This will ensure that security is addressed multiple times, in multiple classes. Furthermore, this could ensure that higher education institutions produce computing graduates that possess fundamental information security knowledge, skills and understanding. This, in turn, will provide computing graduates with the ability to combat information security related threats. This paper briefly reviews existing literature relating to information security in higher education. Furthermore, it explores various South African educators' perspectives on the pervasive integration of information security into undergraduate computing curricula. This was determined through a semi-structured interview supported by a questionnaire. Furthermore, the participants of this research study were educators in the Computer Science, Information Systems, and Information Technology fields. The results indicate that there are various challenges in South Africa regarding the pervasive integration of information security into undergraduate computing curricula.

Keywords

Information Security, Information Security Education, Computing Curricula, Computing Graduates, Pervasive Information Security

1. Introduction

Information as an asset is subject to various security threats, whether deliberate or accidental. The related processes, systems, networks, and people have inherent vulnerabilities which could be exploited by such threats. These threats include viruses, worms, Trojan horses, Denial of Service (DoS) attacks and malware, just to name a few (ISO/IEC, 2013). Information security is the protection of information assets from various threats, which can compromise their confidentiality, integrity, and availability. Whitman & Mattord (2010) suggest that the protection of information cannot only be ensured through the application of security policies, but also through education.

In terms of this research, information security education focuses on providing computing graduates with insight and understanding of information security and should integrate fundamental information security concepts. This research argues towards the pervasive integration of information security into the Computer Science (CS), Information Systems (IS), and Information Technology (IT) fields as this could ensure that these qualifications produce graduates who are capable of pro-active response to information security threats (NIST 2003). The Association for Computing Machinery (ACM), the Association for Information Systems (AIS), and the IEEE Computer Society (IEEE-CS) play an important role in education and curricula development. They state that computing graduates are required to possess information security skills, knowledge, and understanding as they typically will be working with the technological systems of an organisation. Important organisational information is contained in these various systems (ACM/AIS/IEEE - CS, 2005).

Security breaches can occur where different components of a system interface, whether in the interface between different computers in a networked application, or across the interface between the user and the other components of the system. An awareness and understanding of the possible security breaches would give computing graduates the ability to identify and design high-level solutions that are less likely to put the organisation's information assets at risk and that will protect the organisation from various security threats (ACM/IEEE - CS, 2008; ACM/AIS, 2010).

During the deliberations of the Special Interest Group for Information Technology Education (SIGITE) Curriculum Committee, several topics emerged that were considered essential. These essential topics did not seem to belong in a single specific knowledge area or unit and were referred to as pervasive themes. One of these pervasive themes is Information Assurance and Security (IAS) (SIGITE Curriculum Committee, 2005). IAS is intended to protect and defend information and the associated information systems from threats (ACM/IEEE - CS 2013). IAS as a knowledge area should be addressed multiple times in multiple classes (ACM/IEEE - CS, 2008).

One of the ways in which a topic can be integrated as a pervasive theme into multiple knowledge areas or units is with the thread approach. Through the thread approach, pervasive themes can be integrated into the curriculum without changing the essence of the curriculum. Furthermore, individual educators could develop material at their own pace and change the syllabus gradually. This approach would require material on information security to be embedded into the current curricula. By integrating information security as a pervasive theme in multiple knowledge areas or units, students could learn to appreciate the importance of information security as an underlying theme across the curriculum which can help avoid the isolation of knowledge units. Furthermore, the thread approach provides exposure to smaller units of knowledge over a longer period of time allowing students to reflect and better assimilate the basic concepts of information security (Perrone et al. 2005).

Although the ACM defines IAS both as a knowledge area and as a pervasive theme, there is inadequate guidance provided with respect to assisting computing educators in pervasively integrating information security into their various modules (Futcher & Van Niekerk, 2011).

2. Purpose of the study

The main purpose of this study was to determine South African educators' perspectives on pervasively integrating information security into undergraduate computing curricula. This was achieved through addressing four key research objectives. Table 1 depicts the objectives of this research and defines the aim of each.

Research Objectives	
Research Objective 1	To determine computing educators' perspectives on the pervasive integration of information security into undergraduate computing curricula
Research Objective 2	To determine the current integration of information security into curricula
Research Objective 3	To determine which fundamental information security concepts should be integrated into undergraduate computing curricula as a pervasive theme
Research Objective 4	To identify possible approaches for integrating an information security concept into computing curricula and the related challenges

Table 1: Research Objectives

The interview process aimed at achieving the objectives as stated in Table 1. This was supported by semi-structured questions to ensure these objectives were met.

3. Research Process

3.1. Participants

The study included ten participants who were all educators in either CS, IS or IT. These participants were from three universities in the Eastern Cape region of South Africa. Three of the participants were Professors, six were Senior Lecturers, and one participant was a Junior Lecturer. Participation in the study was voluntary.

3.2. Interview Process

A semi-structured interview was conducted with each of the ten participants of this study. The semi-structured interview was supported by a questionnaire. This questionnaire was structured according to the four research objectives as shown in Table 1. At the end of the interview, each of the participants was asked to complete an information security concepts checklist.

The purpose of the checklist was to determine the fundamental information security concepts which should be pervasively integrated into undergraduate computing curricula. When completing the checklist, the participants were encouraged to provide a brief comment as to why they thought the specific concept should or should not be regarded as a fundamental information security concept.

4. Results and Findings

This section presents the results and findings of this study according to the specified research objectives.

4.1. Research Objective 1

The first research objective was achieved through the questions depicted in Table 2.

Question 1	What is your perspective on the importance of information security education to undergraduate computing learners?
Question 2	What is your perspective on the pervasive integration of information security into computing curricula?
Question 3	What is the department/colleagues perspective on the pervasive integration of information security into computing curricula?
Question 4	Has your department ever had a formal discussion regarding information security?

Table 2: Research Objective 1 Questions

From the study conducted, there was general consensus that information security education is important to computing learners and that it should be part of the computing curriculum. In support of this, it was mentioned that information security education is critical from the first to the final year of study. In so doing, it could assist with preparing learners, and most importantly graduates with skills to protect themselves, their personal information, as well as organisational information. Learners need to understand the various threats that exist pertaining to information security in order for them to be able to combat those threats within organisations.

However, despite the general consensus, some participants were not sure as to whether information security should be pervasively integrated into the curriculum. A comment was made that a module should focus on teaching the content of that particular module. In order to be successfully integrated, it needs to be done in a manner that complements the module rather than taking away from the main focus and content of that module. Some participants also felt that it could be difficult for information security to be integrated into certain modules.

Pervasive integration implies that fundamental information security concepts should be taught in multiple modules to ensure that relevant skills, knowledge, and understanding are transferred to the learners across these modules. This, however, was deemed to be unnecessary duplication by some participants. It was suggested that fundamental information security concepts be gradually introduced into the first year to final year modules so that learners understand them better to prevent them from being taught all the concepts at once.

With regards to their colleagues, it was generally agreed that they would consider integrating information security concepts into their modules. However, it was mentioned that in many cases the curriculum was already overloaded and therefore time would not allow for such integration. In some cases, it was thought that information security is addressed in another module within the curriculum.

Some of the participants indicated that many educators may not be aware of the importance of information security in computing education and would, therefore, need to be convinced. However, educators are often resistant to change and would perceive the integration of another topic such as information security into their modules as additional work.

Responses regarding formal information security discussions highlighted that the extent to which this is done varies extensively across the various departments and higher education institutions.

4.2. Research Objective 2

The second research objective was to determine the current integration of information security into computing curricula. Table 3 depicts the three questions related to this research objective as well as the corresponding responses.

Detailed Question		**Yes**	**No**
Question 5	Does the department have a security-related module that is taught to all undergraduate computing learners?	1	9
Question 6	Do you integrate information security into your module?	7	3
Question 6b	If Yes, do you assess information security within your module?	2	5

Table 3: Research Objective 2 Questions

From Table 3 it is clear that most departments do not currently have a specific security-related module that is taught to all undergraduate computing learners. In most cases, this is only done at fourth-year level. One participant mentioned that such a module did exist in their department but that the module was discontinued when the curriculum was changed.

Seven of the participants indicated that they do integrate information security into their module. However, it is only assessed by two participants. It was mentioned that they did not integrate information security because they do not perceive it to be relevant to their module. In certain instances, the educators have already been forced to integrate Human Immunodeficiency Virus (HIV) and Acquired Immune Deficiency Syndrome (AIDS) education into their modules. Some educators understandably would prefer to retain the core focus of their modules.

4.3. Research Objective 3

The third research objective comprised of one question, which was in the form of a checklist of twenty-three information security concepts.

The list of the fundamental information security concepts that should be pervasively integrated into undergraduate computing curricula was derived from the security services and security aspects adapted from the ISO/IEC 7498-2 (1989) standard, Whitman & Mattord (2010), from an analysis of the IAS knowledge area and the related units within the ACM/IEEE-CS in their 'Information Technology 2008, Curriculum Guidelines for Undergraduate Degree Programs in Information Technology' document (ACM/IEEE - CS, 2008) and in the 'Computer Science Curriculum 2013' document (ACM/IEEE - CS 2013). The information security concepts identified include, but are not limited to authentication; confidentiality, integrity and availability; cryptography; digital forensics, disaster recovery, accountability, and privacy.

Nine of the participants completed this checklist.

Question 7	What fundamental information security concepts do you think should be pervasively integrated into undergraduate computing curricula?

Table 4: Research Objective 3 Question

For the purposes of this research, any concept where six or more participants indicated that the information security concept should be pervasively integrated will be regarded as a fundamental information security concept.

In addition, the participants were encouraged to provide a brief comment as to why they think the specific concept should or should not be pervasively integrated into undergraduate computing curricula.

Figure 1 shows the results of Question 7. All participants indicated that authentication, secure principles, secure SDLC and security awareness should be considered as fundamental information security concepts.

However, the concepts of non-repudiation/non-denial, cryptography, intrusion detection, and forensics are considered as non-fundamental concepts. Participants indicated that these concepts should not be pervasively integrated and should rather be taught in more advanced modules, for example, in the fourth year of study. Furthermore, cryptography and digital forensics were seen as specialist areas in industry and, therefore, not required for pervasive integration.

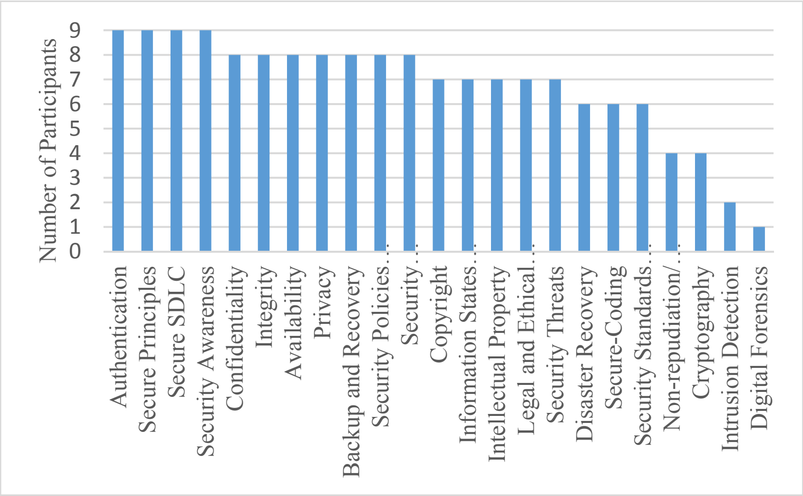

Figure 1: The fundamental information security concepts

As seen in Figure 1, many of the information security concepts were seen by the participants as being important to integrate pervasively into the undergraduate computing curricula.

4.4. Research Objective 4

Table 5 depicts the questions that were asked to achieve the final research objective for this study.

Question 8	Do you have any ideas on how to pervasively integrate information security concepts into various undergraduate computing modules?
Question 9	What challenges do you foresee in the pervasive integration of information security concepts into undergraduate computing curricula?
Question 10	Do you think computing educators would be able to pervasively integrate these fundamental information security concepts into their various modules?

Table 5: Research Objective 3 Questions

Many participants indicated that a good way to integrate information security concepts into particular modules would be to relate or contextualise these concepts to make them as relevant as possible for those particular modules. For example, when teaching Networks, confidentiality, integrity, and availability could be discussed within the context of firewalls and intrusion prevention systems. It is also important to integrate relevant information security concepts that the learners will find interesting. Furthermore, it was suggested that social or interactive discussions related to the students' experience with regard to information security may be beneficial, thereby integrating the concepts through discussion as well as into the theory of the modules. A few of the participants proposed that information security concepts should be pervasively integrated from the first to the final year of study and should be assessed through a capstone-type project towards their final year.

It was also suggested that social media and smartphones, as well as the benefits of security and risks associated with a lack of security, be used as frames of reference to convey certain information security concepts, thereby engaging students through platforms they are familiar with. A further suggestion was that each fundamental information security concept should be covered in at least one of the undergraduate modules. Table 6 below depicts an example of how an information security concept can be pervasively integrated into one or more modules.

Fundamental Concepts	Databases	Programming	Operating Systems	Networks
Privacy	X		X	X
Backup and Recovery	X			X
Security Threats	X	X	X	X
Security Vulnerabilities	X	X	X	X
Legal and Ethical Behaviour	X			X
Confidentiality		X	X	
Integrity		X	X	
Availability		X	X	
Secure coding		X		

Table 6: Mapping of Fundamental Information Security Concepts to Modules

It would be ideal for a single fundamental information security concept to be integrated repeatedly into various modules so that they are taught to learners in multiple classes and multiple times. This could assist the learners in gaining the skills, knowledge, and understanding of these fundamental information security concepts from a different perspective in each module. Many of the fundamental concepts are repeated in other modules as shown in Table 6. In the Database module, for example, the fundamental concepts of privacy, backup and recovery, security threats, security vulnerabilities, and legal and ethical behaviour can be integrated and taught from a database perspective. This could ensure that the concepts complement the module rather than take away the focus and the purpose of that specific module. Similarly, the fundamental concepts that could be integrated and taught from a Programming, Operating Systems, and Network perspective are shown in Table 6. It was also highlighted by many participants that for any of these ideas or strategies to work, educators must be motivated and willing to integrate these information security concepts into their particular module.

The challenge that all participants highlighted was that there is often not enough time to work through current module content and if additional content, for example, information security concepts, needed to be included, this would prove very challenging. It was suggested that the planning of how and where these concepts would be integrated should be done at the beginning of each year to ensure that each concept is addressed multiple times in multiple modules. Furthermore, a few of the participants indicated that a challenge to pervasively integrating information security concepts into various modules may be resistance from educators as they are reluctant to change, and their 'buy in' would be necessary for the pervasive integration to be successful. It was also suggested that educators may be unaware, or lack knowledge, regarding information security concepts, or may not be confident in teaching these concepts. Therefore, it was suggested that, in order to facilitate their integration, the fundamental information security concepts should be provided to educators in a format that would make it easy for them to understand and convey to learners.

Most participants indicated that there would, most likely, be resistance to the added workload required to integrate the information security concepts into modules and that educators are, for the most part, resistant to change. One participant indicated that he did not think that educators would be able to integrate these fundamental security concepts into their modules and it would depend on what the educators would have to do. To assist with this, it was suggested that examples of how educators could integrate these concepts into their modules and how to make these examples relevant to their specific module and context would benefit educators, particularly those whose modules are not security focussed. However, the participants also indicated that educators would need to be convinced that the integration of information security concepts is necessary and it would be important to show educators the value of information security education, to increase their willingness to integrate these concepts into their modules.

5. Conclusion

Information security is a fundamental and common topic that can fit into any computing module. However, the appropriate information security concepts should be identified for each specific module to ensure the effective integration of these information security concepts into the various computing modules. This will ensure that computing graduates are equipped with the required information security skills, knowledge, and understanding. The primary aim of this study was to determine South African computing educators' perspectives on the pervasive integration of information security into computing curricula. This was achieved through the four research objectives specified in Section 2. The results and findings from this study indicated that these computing educators are aware of the importance and generally support the pervasive integration of information security into undergraduate computing curricula. However, they do not currently integrate information security effectively into their various modules. Many computing educators still need to be made aware of the importance of information security education to computing learners and they require assistance to ensure the effective integration of these information security concepts into the various modules. Thus, further research is required to determine how these fundamental information security concepts can be seamlessly integrated into the various computing modules. The limitations of this study are that this study was an exploratory study conducted in South Africa. Generalization of the study's findings to other countries cannot be ensured.

6. Acknowledgements

The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors, and are not necessarily to be attributed to the NRF.

7. References

ACM/AIS, 2010. IS 2010: Curriculum guidelines for undergraduate degree programs in information systems. *Communications of the Association for Information Systems*, 26, pp.359–428.

ACM/AIS/IEEE - Computer Society, 2005. Computing Curricula 2005. *ACM Journal of Educational Resources in Computing*, 1(3), pp.1–240.

ACM/IEEE - Computer Society, 2008. Information Technology 2008 Curriculum Guidelines for Undergraduate Degree Programs in Information Technology. *Current Practice*, pp.1–139.

ACM/IEEE - CS, 2013. Computer Science Curricula 2013. *Practice*, pp.1–172.

Futcher, L. & Van Niekerk, J., 2011. Towards a Pervasive Information Assurance Security Educational Model for Information Technology Curricula. In F. Ronald C, Dodge Jr & Lynn, ed. *Proceedings of the 7th World Information Security Education Conference*. Lucerne, Switzerland: Springer Berlin Heidelberg, pp. 47–54.

ISO/IEC 27002:2013, 2013. *ISO / IEC 27002 Information technology — Security techniques — Code of practice for information security controls* 2nd ed., Switzerland: ISO.

ISO/IEC 7498-2, 1989. *Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2 : Security Architecture*, Switzerland: ISO/IEC.

NIST, 2003. Building an Information Technology Security Awareness and Training Program. *NIST SP 800-50*, (October), pp.1–38. Available at: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

Perrone, L.F., Aburdene, M. & Meng, X., 2005. Approaches to undergraduate instruction in computer security. *2005 ASEE Annual Conference and Exposition: The Changing Landscape of Engineering and Technology Education in a Global World*, pp.651–663.

Special Interest Group on Information Technology Education Curriculum Committee, 2005. *Computing Curriculum Information Technology Volume*,

Whitman, M.E. & Mattord, H.J., 2010. *Management of Information security* 3rd ed., Course Technology, Cengage Learning.