Information Security Education: Bridging the gap between academic institutions and industry

1Prof. E. Smith, 2Mrs E. Kritzinger, 3Prof. H.J. Oosthuizen and 4Prof.S.H. von Solms

1&2School of Computing, University of South Africa, PO Box 392, UNISA, 003, South Africa.

3 School of Computational and Mathematical Sciences, University of the North, Private Bag X1106, Sovenga, 0727, South Africa.

4 Standard Bank Academy for Information Technology, Rand Afrikaans University, PO Box 524, Auckland Park, 2006, South Africa.

Abstract

Information Security has been established as a growing discipline around the globe. There is however, a shortage of Information Security professionals in industry and a lack of Information Security awareness in organizations. This results in a real need for Information Security education. Additionally it is essential that the academic sector incorporates the needs of industry when teaching Information Security. This paper is devoted to an investigation of Information Security Education with a view to define a common body of knowledge for Information Security that incorporates the needs of both industry and the academic sector. The purpose of the paper is to propose a framework that maps the Information Security needs of industry to the academic sector. The framework could be used as a starting point when developing an Information Security education program.

Keywords

Information Security Education, Information Security Curricula, Information Security Education Programs, Common Body of Knowledge for Information Security.

1. Introduction

The rapid development of Information Technology (IT) creates a real concern for Information Security. According to the CSI/FBI Computer Crime and Security Survey (2003), technological innovations such as the World Wide Web and the Internet increase the occurrence of information related crimes. Information Security has therefore become a fundamental factor for the growth and success of almost all organizations. One of the primary concerns with regard to Information Security is the huge shortage of Information Security professionals. According to Thomson and von Solms (1998) the user profile has changed form a situation where all users were computer or information technology specialists to a situation where most users today are barely computer literate. Wright (1998) argues that insufficient education has led to this problematic situation. There is therefore a clamant need for Information Security professionals with a sound knowledge of the fundamentals of Information Security and with an ability to apply this knowledge in the ever-changing field of Information Security (Bishop, 2000; Hancock, 2001; Irvine, Chin & Frincke, 1998 and Wright, 1998).

Educational institutions and researchers have responded to this need by initiating security related research and proposing Information Security education programs and curricula (Armstrong & Jayaratna, 2003; Cockroft, 2003; Grimaila, 2003 and Surendran, Kim & Harris, 2003). According to Bishop (2000) all forms of education are critical to address and improve the need for Information Security professionals. Integrating Information Security into more areas of Computer Science education at *academic* institutions is one form of education that would present an improvement to the shortage of educated professionals in the field of Information Security. Providing education to *industry* would also address this shortage. The Global Information Security Survey of 2003 reported that only 35 % of organizations had continuous Information Security education and awareness programs in place (Assurance and Advisory Business Services, 2003). This is a serious concern, because employees ought first to be educated and made aware about Information security issues before they can be held accountable for their actions.

The purpose of this paper is to investigate Information Security Education with a view to propose a framework that maps the Information Security needs of industry to the academic sector. The first part of the paper is devoted to an investigation of the status of Information Security education. It presents findings of a South African survey conducted among all Universities in South Africa regarding Information Security education. It also provides an overview of some of the prominent research activities regarding Information Security education conducted globally by both the academic and the industry sectors. The second part of the paper is devoted to defining a Common Body of Knowledge (CBK) for Information Security. The paper culminates in presenting the framework that could be used as a starting point when developing an Information Security education program.

**2. Status of Information Security Education**

**2.1 The Academic Sector**

Educational institutions worldwide have responded to the need for educated Information Security professionals by conducting research with regard to Information Security Education. The first part of this section reports on the results of a South African survey conducted among all Universities in South Africa, whereas the second part of this section is devoted to an overview of some of the prominent research activities conducted globally with regard to Information Security Education.

* + 1. South African study

The authors conducted a survey to determine the status of Information Security Education at tertiary institutions in South Africa. The method of research comprised the use of a questionnaire. The questionnaire consisted of six sections. Due to the length of this paper the questionnaire is not included and we therefore provide a brief explanation of the contents of the questionnaire.

The first section of the questionnaire recorded personal details of the participant such as his/her name, name of the University, name of the School/Department and current rank. The second section recorded information on all undergraduate Information Security courses offered. This included information such as the name of the course, the duration of the course, the Information Security topics covered by the course, the average number of students that enroll for the course and the average pass rate. The third section of the questionnaire recorded similar information for all postgraduate Information Security courses offered (Honours, Masters & Doctorate). The questionnaire further distinguished between Masters degrees consisting of full dissertations and those consisting of lectured courses combined with a dissertation of limited scope. The fourth section of the questionnaire recorded information where Information Security courses are offered for non-degree purposes. The fifth section provided space to enter any relevant additional information not recorded elsewhere in the questionnaire, whereas the last section dealt with the scenario where no Information Security courses are offered at all.

The questionnaire was distributed electronically as far as possible. In this way we hoped to obtain a high response. Completion of the questionnaire was voluntary, but not anonymous. Since syllabi are in the public domain the content of this questionnaire is not regarded as confidential. The results are, however, presented in such a way that the names of the Universities that were included in the sample are not connected directly to the information displayed.

The questionnaire was distributed to all, i.e. 24, Universities in South Africa. 16 Universities combine Information Systems and Computer Science into one School/Department, whereas the remainder of 8 Universities has a separate School/Department for Information Systems and Computer Science (which might also be in different faculties). There are therefore 32 Schools/Departments among the 24 Universities. The names of the Universities as well as the different Schools/Departments are listed in Appendix A. (In 2004 some Technikons and Universities in South Africa have been merging. The questionnaire was distributed at the end of 2003 before the merging process. At that stage South Africa had a total of 24 Universities.)

The data obtained from the survey represents 24 Schools/Departments. In other words 24 out of 32 Schools/Departments completed the questionnaire, which represents a response rate of 75%. The results presented therefore, only depict information on the 24 Schools/Departments that completed the questionnaire. It is important to note that we present the results according to individual Schools/Departments – not Universities. The Statistical Package for Social Scientists was used to analyze and graphically depict the data. Due to paper length, we only included those results that are most relevant to the purpose of this paper.

Figure 1 depicts the percentage of Schools/Departments that offer Information Security (at any level). This includes stand-alone Information Security courses, as well as those Information Security courses offered implicitly as part of another course. The majority of Schools/Departments i.e. 75%, therefore offer Information Security at some level. Note, however, that these figures do not give an indication of the *number* of Information Security courses offered by a specific School/Department.



**Figure 1: Schools/Departments that offer Information Security (IS)**

Figure 2 additionally depicts that 63.2% of these Schools/Departments offer Information Security as a stand-alone course as opposed to 36.8% that offer Information Security implicitly as part of other courses.



**Figure 2: Schools/Departments offering Information Security (IS) as a stand-alone course**

Based on information captured by the questionnaire we made the following observations:

* Many of the rural Universities are more focused on educating students about issues relevant to their direct environment instead of issues relevant to industry.
* There are insufficient lecturers with adequate Information Security knowledge to present Information Security courses.
* The Information Security topics covered in courses where Information Security forms an implicit part of the course, represent only a small part of the fundamental Information Security topics.
* As stated earlier, 36.8% of Schools/Departments offer Information Security implicitly as part of other courses. Some of these courses form part of the curricula of other disciplines (such as Accounting or Philosophy) although the School of Computer Science/Information Systems offers them. This indicates that Information Security courses should be formulated in such a way that multidisciplinary students benefit from the course.

2.1.2 Global Information Security Education research

In 1998 a similar study to the South African study was conducted in the United States (Wright, 1998). At that stage only a few Universities in the United States were meeting the need for Information Security education. Only a few American Universities or colleges offered in-depth education in this field. Those Universities that taught Information Security courses focused on a narrow domain of this field only. Furthermore, the US military was the source of most funding opportunities, and therefore academic research tended to focus on military security requirements. Specialized attention was given to technical details and scant attention was paid to the non-technical business Information Security issues.

In 1999 Cohen investigated a number of issues with regard to Information Security Education, such as distance learning advantages and limitations and delivery mechanisms for educational materials (Cohen, 1999). He realized that the field of Information Security is unique because it seems to be changing at a very rapid pace and there is an enormous market need for expertise and a lack of University curricula in the field.

In 2001 Schlarman identified three elements that should be the core of every Information Security program, namely people, policies and technologies (Schlarman, 2001). He explored how these three elements should interact with one another to strengthen an Information Security program. Another prominent development in Information Security education during 2001 involved the work conducted by Yang (Yang, 2001). Yang investigated the impact of Information Security on Computer Science education. He argued that Information Security curricula should include ethical and cultural issues and should also address technical, business and managerial aspects. In the same line Grimaila and Kim (2001) identified the following three aspects that a typical Information Security professional should be familiar with:

* Research, development and application of technical principles;
* application of industry accepted techniques and practices and
* non-technical aspects such as policy development, resource allocation and risk assessment and management.

During 2002 Caelli investigated a number of security challenges, including the burning issue whether education kept up with security requirements by industry. He expressed the concern that the current generation of IT managers had little to no formal educational exposure to Information Security principles or technology (Caelli, 2002). In 2002 Anderson and Schwager also conducted a survey with regard to Information Security. The outcome of the survey indicated that Information Security should ideally be integrated into all other courses in the curriculum.

Finally, various tertiary institutions have developed one or more courses in Information Security at undergraduate or postgraduate levels (Armstrong & Jayaratna, 2002; Cockroft, 2002 and Grimaila & Kim, 2001).

Based on the outcome of the South African study and the other globally research activities regarding Information Security Education, the authors identified the following three issues that are of primary concern for the academic sector:

* There is a *need for Information security professionals* (Cohen, 1999 and Caelli, 2002)*;*
* Information Security education programs should strike a *balance between* *technical and non-technical aspects* and
* Information Security Education should keep up with *security requirements by industry*.

The next section explores the needs of industry with regard to Information Security Education.

**2.2 The industry sector**

An Information Security education program should also adhere to the expectations of industry (Bishop & Frincke, 2003; Caelli, 2002 and Grimaila & Kim, 2001). A number of standards and codes of practices exist to serve as baseline for organizations when implementing or managing Information Security, for example the British standard for Information Security Management BS7799/ISO17799 (Barnard & von Solms, 1998; BS 7799, 2003; Department of Trade and Industry, 1995; ISO17799, 2002 and von Solms & von Solms, 2001), the Generally Accepted System Security Principles (GASSP) document (Grimaila & Kim, 2001 and International Information Systems Security Certifications Consortium, Inc. (ISC)2, 2002), Control Objectives for information and Related Technologies (COBIT) (COBIT, 2001; Van GremBergen, 1997 and Ward & Smith, 2002) and Guidelines for the management for Information Technology Security (GMITS) (GMITS, 2001 and von Solms, 1998).

The BS7799 – now also known as ISO 17799 – is arguably the leading international Information Security management standard in industry, as it provides an internationally accepted scheme against which an organization can be evaluated and certified in terms of its Information Security. The next section is devoted to a discussion of this standard.

2.2.1 BS7799

The British Standards Institution published the BS7799 standard in February 1995. This Code of Practice for Information Security Management was based on a document published by the Department of Trade & Industry (the DTI) in 1993 (Buzard, 1999; Department of Trade and Industry, 1995; Kearvell-White, 1996 and Quinn, 1997). The aim of the BS7799 standard is to:

* Provide a common basis for organizations to develop, implement and measure Information security management practice and to
* provide confidence in inter-organisational business ( Department of Trade and Industry, 1995).

The BS7799 standard consists of two parts (Buzard, 1999; Kearvell-White, 1996 and Lillywhite, 2004). Part 1: 1995 is now known as ISO/IEC17799:2000. This Part provides guidance to assist companies in implementing an Information Security system. It designates ten key controls which are either “essential requirements…or are considered to be fundamental building blocks for computer security…”, namely (Keravell-White, 1996):

* Information security policy document
* Allocation of information security responsibilities
* Information security education and training
* Reporting of security incidents
* Virus controls
* Business continuity planning
* Control of proprietary software copying
* Safeguard of organizational records
* Data protection
* Compliance with security policy

Part 2 (BS7799-2:2002) of the BS7799 standard is the requirements specification against which an organization can be evaluated for compliance and subsequent certification.

Having highlighted some of the prominent research activities regarding Information Security Education in the academic and industry sectors, it becomes evident that the development of information security education programs is essential and remains an urgent and complicated task. The first step in developing such a program is to define a Common Body of Knowledge (CBK) for Information Security. In the next section the authors aim to define a CBK for Information Security that incorporates the needs of both industry and the academic sector.

**3. A Common Body of Knowledge for Information Security**

Having examined the status of Information Security Education, the authors realize that Information Security education programs should keep up with needs of industry. Additionally, the domain of Information Security is no longer exclusively of a technological nature, but includes aspects of human behavior. According to Siponen (2000), even though the human component has been recognized as playing a crucial role in Information Security, the human issues have not received much attention. The discussions in this paper confirm that non-technical issues (or human issues) should form an integral part of any Information Security Education program. As mentioned earlier defining a CBK for Information Security forms the cornerstone of an Information Security Education program.

The authors define a CBK for Information Security that divide Information Security topics into two broad areas, namely technical aspects of Information Security and non-technical aspects of Information Security. In this way the authors aim to ensure that the human issues are taken into account when developing an Information Security Education program. Consider Figure 3.

**Technical Information Security Aspects**

Firewalls

Intrusion detection

Passwords

Encryption

Access control

Database security

…

**Non-Technical Information Security Aspects**

Security policies

Legal aspects

Corporate governance

Ethics

Awareness

Contingency planning

…

# Figure 3: CBK for Information Security

The technical aspects of Information Security focus primarily on the technical oriented knowledge and tools that are required to secure and protect information – such as firewalls. These aspects are technical in origin and are usually only confined to the technical departments and employees in organizations. The non-technical aspects of Information Security on the other hand, include all the non-technical oriented knowledge and tools such as ethics, legal issues and Information Security awareness. The focal area of the non-technical aspects is the different influences humans could have on information. These human influences can be classified as either intentional or accidental and can originate internally or externally to an organization.

Note that the list of non-technical and technical Information Security aspects depicted in Figure 3 is not complete, but is sufficient for illustrating the concept. There are a number of International and national Information Security documents available as mentioned earlier in Section 2.2 – such as the British standard for Information Security Management BS7799/ISO17799, Control Objectives for information and Related Technologies (COBIT) and Guidelines for the management for Information Technology Security (GMITS) – that should be consulted to determine an exhaustive list of Information Security topics that should form part of the CBK for Information Security. These documents consist of a vast amount of knowledge regarding the management and implementation of Information Security in an organization.

**4. The Framework**

In order to present a framework that maps the Information Security needs of industry to the academic sector, it is essential to determine those information security aspects (that form part of the CBK of Information Security) that each of the authority levels or “role players” in an organization should be familiar with. According to National Institute of Standards and Technology (1998) there are many different ways to identify individuals or groups who need specialized or advanced training. One approach is to consider job categories, such as executive, functional, managerial or technological. Another approach is to consider job functions, such as system design, system operation, or system use. A third approach is to consider the specific technology and products used. The authors used the first approach (i.e. job categories) to identify the different authority levels (“role players”) in a typical organization.

The authority levels will differ from organization to organization, depending on their internal structure. Each authority level is required to know, understand and implement different information security aspects in their day-to-day activities. An example of authority levels in a typical organization is:

* Board Level
* Executive Management Level
* Technical Management Level
* Security Management Level
* User Level

Since each authority level has different information security responsibilities it is vital that the Information Security education program incorporates this differentiation. Academic institutions should accordingly structure their education programs in such a way that it addresses specific authority levels in industry. However, this is easier said than done, because there are numerous ways of grouping specific Computer Science and Information Systems topics together.

Consider Figure 4 that depicts an example of the proposed framework that maps these needs of industry to the academic sector. The International/National Information Security documents that contain information on Information Security management and implementation should first be consulted to determine the CBK for Information Security. The CBK is divided into technical and non-technical Information security topics – as discussed earlier. Each authority level of a typical organization is accordingly required to understand and implement one or more topics of the CBK. The arrows in Figure 4 represent the mapping of specific Information Security topics to specific authority levels and accordingly to suitable academic subject streams.

In our example, the Board level should be educated in legal aspects, Corporate Governance issues, risk management, ethics and security policies. A typical academic institution should therefore include these topics of the CBK into one or more of their subject streams, in this case into their Business management stream. Similarly for the Executive Management level.

The Technical Management level should be educated in firewalls, encryption techniques, network security and the implementation of passwords. These topics should be distributed between the Programming and the Network streams of an academic institution.

Furthermore, the Security Management Level is ultimately responsible for safeguarding the assets of an organization (National Institute of Standards and Technology, 1989). This authority level is therefore responsible to ensure that all necessary information security control measures are implemented to prevent information security breaches in the organization. The Security Management Level should accordingly be educated in topics such as risk management and security policies and these topics should be distributed between the Business management and IT management streams of an academic institution.

Finally, the User level of a typical organization should be educated in ethics, security policies and the use of passwords and these topics should be included into the End user computing stream of an academic institution.

Board

Executive Management

Technical Management

Security Management

User

###### International/National Information Security documents

**ACADEMIC:**

**Subject stream**

Business management

IT management

Programming

Networks

End user computing

**INDUSTRY:**

**Authority levels**

Board

Executive Management

Technical Management

Security Management

User

**CBK for Information**

**Security professionals**

**Non-technical** topics of Information Security

Legal aspects

Corporate Governance

Risk management

Ethics

Security policies

…..

**Technical** topics of Information Security

Firewalls

Encryption

Network security

Passwords

…….

# Figure 4: Framework for mapping needs of Industry to the academic sector

From the above example it is clear that the Information Security needs of industry should determine the content of academic Information Security programs. Note however, that this is not an elementary process, because Information Security could also be offered implicitly as part of other streams that are not included in the Computer Science or Information Systems departments.

**5. Conclusion**

There is a growing international need for more Information Security professionals as well as a need to step up the level of Information Security awareness among employees. This paper focused on Information Security education and highlighted the need for incorporating the Information Security requirements of industry into the academic sector. The authors accordingly defined a Common Body of Knowledge (CBK) for Information Security that divides Information Security into technical and non-technical aspects. The last section of the paper was devoted to a presentation of a framework that maps the Information Security needs of industry to the academic sector using the CBK for Information Security. It is envisaged that this framework should provide a sound foundation for guiding the development of a typical Information Security education program. The development of an Information Security education program is, however, an on-going process and such a program should therefore be constantly revised to ensure that it remains up to date with international standards and practices as well as with the expectations from industry.

**6. References**

CSI/FBI Computer Crime and Security Survey. 2003. Available online at <http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf>. Accessed on 2004/10/29.

Anderson, J.E. & Schwager, P.H. 2002. Security in the information systems curriculum: identification & status of relevant issues. *Journal of Computer Information Systems*, 42(3): 16-24.

Armstrong, H.& Jayaratna, N. 2002. Internet Security Management: a joint postgraduate curriculum design. *Journal of Information Systems Education*, 13 (3):249-258.

Assurance and Advisory Business Services. 2003. Global Security Survey. Available online at [www.ey.com](http://www.ey.com). Accessed on 2004/09/29.

Barnard, L. & von Solms, R. (1998). The evaluation and certification of information security against BS 7799. *Information Management & Computer Security*, 6(2): 72-77. UK: MCB University Press.

Bishop, M., 2000. Education in information security. *IEEE Concurrency*, 4-8.

Bishop, M. & Frincke, D. 2003. Who watches the security educators? *IEEE Security & Privacy*, 56-58.

BS 7799. (2003). BS 7799 – slow uptake by companies. *Computer Fraud & Security*, 3: 3. UK: Elsevier.

Buzzard, K. (1999). Computer security – What should you spend your money on? *Computers & Security*, 18: 322-334. Elsevier Science Ltd.

Caelli, W.J. 2002. Trusted…or…trustworthy: the search for a new paradigm for computer and network security. *Computers & Security*, 21(5): 413-420.

COBIT – Governance, Control and Audit for Information and Related Technology. (2001). IT Governance Institute / ISACA / ISACF, 3rd edition.

Cockroft, S. 2002. Securing the commercial Internet: Lessons learned in developing a postgraduate course in information security management. *Journal of Information Systems Education*, 13 (3):205-210.

Cohen, F. 1999. Managing network security: Security Education in the Information Age. *Network Security*, 10: 7-10.

Computing curricula 2001. Available online at <http://www.computer.org/education/cc2001/final/index.htm>. Accessed on 2004/02/09.

Department of Trade and Industry. (1995). Accredited certification against BS7799. *Computer Audit Update*, 9: 18-19. Elsevier Science Ltd.

GMITS: Guidelines for the Management of IT Security, Part 1: Concepts and models for managing and planning IT security. (2001). ISO/IEC JTC1/SC27, PDTR 13335-1 (revision), version 28-11-2001.

Grimaila, M.R. & Kim, I. 2001. An undergraduate business information security course and laboratory. *Journal of Information Systems Education*, 13 (3): 189-195.

Hancock, B. 2001. Security Views. *Computers & Security*, 20:278-294.

International Information Systems Security Certifications Consortium, Inc. (ISC)2 2002. Common Body of Knowledge (CBK). Available online at <http://www.isc2.org/cgi/content.cgi?page=30>. Accessed on 2004/02/20.

Irvine C.E., Chin S.K. & Frincke D. 1998. Integrating Security into the Curriculum*. IEEE Computer,* 25-30.

ISO17799. (2002). Information security management systems - specification with guidance for use*,* British Standards Institute (BSI), final draft BS7799-2: 2002.

Kearvell-White, B. (1996). National (UK) computer security survey 1996. *Information Management & Computer Security*, 4(3): 3-17. UK: MCB University Press.

Lillywhite, T.P. (2004). Implementing BS7799 in the UK National Health Service. *Computer Fraud & Security*, 2004(2): 4-13. Elsevier.

National Institute of Standards and Technology (NIST). 1989. Computer Security Training Guidelines. Available online at [www.nist.gov/](http://www.nist.gov/). Accessed on 2004/10/20.

Quinn, M. (1997). Do you know the security code? *Computers & Security*, 16(2): 129. Elsevier.

Schlarman, S. 2001. The People Policy, Technology (PPT) model: core elements of the security process. *Information Systems Security*, 10(5): 36-41.

Siponen M.T. 2000. Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice. *Information Management & Computer Security*, 8:5.

Surendran, K., Kim, K. & Harris, A. 2002. Accommodating Information Security in our curricula. *Journal of Information Systems Education,*  13 (3): 173-176.

Thomson M.E, & Von Solms R. 1998. Information security awareness: educating your users effectively*. Information Management & Computer Security,*  6(4): 167-173.

Van Grembergen, W. (1997). Millenium conversion & COBIT. *Computer Audit Update*, Jul 1997: 17-24. Elsevier Science Ltd.

Von Solms, B. & von Solms, R. (2001). Incremental information security certification. *Computers & Security*, 20(4): 308-310. Elsevier Science Ltd.

Von Solms, R. (1998). Information Security Management (2): guidelines to the management of information technology security. *Information Management & Computer Security*, 6(5): 221-223.

Ward, P & Smith, C.L. (2002). The development of access control policies for information technology systems. *Computers & Security*, 21(4): 356-371. Elsevier Science Ltd.

Wright, M.A. 1998. The need for Information Security Education. *Computer Fraud & Security*, 14-17.

Yang, T.A. 2001. Computer security and impact on Computer Science education. *JCSC*, 16(4): 233-246.

Appendix A

List of South African Universities (2003):

|  |  |
| --- | --- |
| **University** | **School/Department** |
| Bond South Africa | Computer Science |
| Cape Town | Computer Science  Information Systems |
| Durban-Westville | Computer Science  Information Systems |
| Fort Hare | Computer Science |
| Medunsa | Computer Science |
| Monash | Computer Science & Software Engineering |
| University of Natal | Computer Science  Information Systems |
| Newport | Business Administration |
| North | Computer Science & Information Systems |
| North-West | Computer Science |
| Orange Free State | Computer Science |
| Port Elizabeth | Computer Science & Information Systems |
| Potchefstroom | Computer Science & Information Systems |
| Pretoria | Computer Science  Information Systems |
| Rand Afrikaans | Standard Bank Academy for IT |
| Rhodes | Computer Science  Information Systems |
| Stellenbosch | Computer Science |
| Transkei | Computer Science  Information Systems |
| Unisa | Computing |
| Venda | Computer Science & Information Systems |
| Vista | Computer Science & Information Systems |
| Western Cape | Computer Science  Information Systems |
| Witwatersrand | Computer Science  Information Systems |
| Zululand | Computer Science |