https://doi.org/10.48009/2_iis_2009_185-193

INTRODUCING A CONCENTRATION IN INFORMATION ASSURANCE INTO A COMPUTER SCIENCE PROGRAM

Azad Ali Indiana University of Pennsylvania azad.ali@iup.edu
Waleed Farag, Indiana University of Pennsylvania, farag@iup.edu

ABSTRACT

The purpose of this paper is to illustrate the experience of one department at introducing a program in information assurance. The department of Computer science (COSC) at Indiana University of Pennsylvania (IUP) has been offering a Bachelor of Science degree (B.Sc.) in Computer Science Information Assurance Track for several years. The development of this degree and their contents has been implemented to respond to various demands including the nation's needs for trained security professional as well as the Information Technology (IT) sector market. The content of this program has taken different factors regarding to faculty availability, technological need and market demand. The experience of this computer science department in developing the Bachelor of Science degree in information assurance is illustrated in this paper. The paper first reviews literature regarding the evolving information assurance over all and in academic programs in particular. Then, it focuses on the experience of the Computer Science department at Indiana University of Pennsylvania in introducing a track in information assurance within their program.

Keywords: Information Security, Information Assurance, Concentration of Information Assurance Program, Information assurance and computer science program

INTRODUCTION

Academic technology programs repeatedly and continuously change their curriculum. Different reasons are attributed to these continuous changes in computer technology programs, but responding to market demand is one of the prime factors that lead computer programs to update their curriculum.

Electronic exchange of data led to the simplification and to the abundance of sharing information across different platforms and media. This however left a lot of information to be vulnerable and made them subject to be exploited in different unintended ways. This kind of exploitation created a necessity to establish procedures and technologies that guard the information from unintended use [8]. People had to be trained on the technologies and procedures that have alluded to the exploitation that was mentioned above to be able to halt information from being exploited. As a result, a gap in the market has been created for people who are trained in guarding against exploitation and misuse of information and also to set guidelines for such practices. This sets the stage for creating a profession for such people. The name of this profession is termed "information security" or "information assurance".

Academic institutions worked to fill this gap in the industry by offering programs that train students specialized in information security or assurance [1]. One of these programs is developed by a university located in Western Pennsylvania. The department of computer science (COSC) at Indiana University of Pennsylvania (IUP), in collaboration with the Criminology Department, has started a program that offers a Bachelor of Science degree in information assurance. The experience of this program is illustrated in this paper.

The remainder of the paper is divided into four sections. The first section defines information assurance and provides a brief history of its use. The second section discusses the development of information assurance programs in computer academic curriculum. The third section elaborates on the factors that contribute to the success of introducing a new academic program in general. The fourth section illustrates the experience of IUP at introducing their degree program in information assurance. A summary and suggested future study is included at the end.

ABOUT INFORMATION ASSURANCE

The term "information assurance" is not new. It has been used at various business, public and private forums. It has been also used widely in academic institutions for some time. However, the context within which the term has been used has changed lately to include a wider range of criteria and factors. At the same time, the information security field of study has been modified to reflect the most recent inclusion of technological changes and the resultant increase of exchanging of private and public information. Thus a discussion of the meaning, development and content of this term is warranted. The remainder of this section introduces definitions of this term, a brief history of their use at private and public institutions.

Information Security - Definition

"Information Assurance" means different things to different people. The same term is used along with other terms like information security, computer security and network security.

Various definitions have been reported regarding information Assurance/security. For example, Leeuw and Bergstra [12], explained information secuirty from the perspective of a system and noted that infomation security means:

> "The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authrized users. Information security include those measures necessary to detect, document, and counter such threats P. 2".

Innella [10] used the term Network Security and explained that it refers to hardware, functions, characteristices, features, operational procedures, accountability measures, access controls, and administrative and management policy required to provide an acceptable level of protection for hardware, software and information in a network.

From the definitions outlined above, it can be noted that authors used the term "Information Assurance", "Information Security" and "Network Security" to denote same functions and procedures. In this paper, we are going to use the terms "information security" and "information assurance" interchangeably to mean the same thing. So at times we may refer to "Information Security" more often because it is referenced more frequently in academic programs, but the meaning is going to be the same as it applied to "Information Assurance".

Information Security – A Brief History

The history of information security is not recent, and dates back to many years ago. Leeuw [12] notes that "The history of information security does not begin with the advance of telegraph, the wireless (p. 1)". The same author further divided the development of information security into five stages:

1. Intellectual ownership: This is when the scientific information became widely acknowledged and the need rose to safeguard this knowledge from being acquired or used by others without having the prior authorization.

2. Identity Management: Modern states need to know how its citizens and banks have knowledge about their customers. Thus they need to collect information about clients, customers, patients, citizens and others.

3. Communication Security: Communication security ranges from encrypting letters that are sent via mail or to classified information that are sent via other communication lines.

4. Computer Security: The introduction of time-sharing and multi-tasking made it difficult to strictly classify information in high degrees of confidentiality.

Privacy – and Regulations: The abundance of information about citizens led to regulations that identify private information and guard against distributing them without permission.

Innella [10] on the other hand explained that the introduction of the Internet provided the spark which led to increasing the use of Information security. The same author noted further that in 1969 the Defense Advanced Research Project Agency (DARPA) solicited the effort of other institutions to design a network through which data could be passed and received. Some of these data were sensitive and this in turn led to establishing procedures for sharing sensitive information on the network and device technology to protect the information from being stolen.

Although introducing the Internet led to increase the sharing of information which in turn increased the use of information security, the swell of information security programs at academic institutions was not witnessed until the turn of the century. The wide spread use of business transactions electronically placed more urgency on delivering this information accurately. This in turn added to the importance of finding people who can protect this information from being tampered with. Academic programs realized this need and started different programs and courses to train people to acquire such skills.

Information Security and Academia

According to Innella [10], securing computer networks had its roots in 1960s when computers were connected through dumb terminals via networks and information exchanged through the network. Computer academic programs started initially teaching computer security in small doses, in a chapter or a few chapters in a book or through covering it with other topics in the same course. Later development increased the volume at which information security is taught at academic programs. In these days, nearly all computer programs have at least one course or topic that is devoted to teaching computer or information security in one form or another. Often an entire degree is devoted to teaching information security.

The best way to show how information security programs progressed in academic curriculum is to review some of the standard curricula and carefully observe how much coverage was suggested in each of these curricula. Standard curricula like CC2001, IS2002, and CC2005 are established to provide suggestions on what to include in each respective curriculum. The following section explains the extent of coverage of information security in each of the standard curriculum. It first lists the name of the standard curriculum, a brief description of what program it entails and then covers the extent at which the coverage of information security is included in the same curriculum.

ABOUT STANDARD CURRICULUM

There are a number of organizations that work to develop standards for various technology fields: The Association for Computing Machinery (ACM), the Institute of Electrical and Electronics Engineers (IEEE), the Association of Information Systems (AIS) and the Association of Information Technology Professionals (AITP). These organizations have worked at many levels to develop standard curriculum for different computer disciplines. They have developed a number of documents in this regard and have indicated that they will continue to do so to develop additional documents as the need for developing such documents arises. The initial focus of these efforts was to develop a standard curriculum for the computer science majors. This evolved into a larger number of standard curricula to cover wider range of computer related programs.

The documents that are developed by these organizations are labeled as computing curriculum, though not officially considered “standards”; they have been widely used in curriculum development and accreditation. In fact, due to their wide use in higher education, these documents are considered as de facto standard curriculum in the computing technology fields.

CC2001

The computing curricula 2001 (CC2001) pertains programs in computer science discipline. This was the second standard curriculum regarding this discipline; the first one was developed in 1991. CC2001 was developed after the turn of the century where the computer industry witnessed a lot of changes and also the appearance of other new disciplines in the computer field like Information System and Information Technology.

The CC2001 document listed first the technical changes that has led to creating this volume and listed "topics of importance of many curricula" within its' content. There are 12 such topics listed in CC2001; among these topics is "Security and cryptography".

CC2001 included a figure that contains Computer science body of knowledge with core topics. This figure is divided into 14 body of knowledge, each has different topics. Each body of knowledge can serve to be one course in such a curriculum. There was no one body of knowledge that is assigned entirely to computer or information security. However, under the "Operation System" body of knowledge, Security and protection was listed as one suggested topic of coverage. Network security was also listed as a topic under the Net-Centric Computing body of knowledge. Furthermore, network security was noted in CC2001 as one of the "recurring themes" from the earlier 1991 version of the computer curriculum.

IS2002

This is the information systems volume of the standard curriculums. It is the second volume that is developed for the information systems field, the first one was developed in 1997.

IS2002 included a table titled "Representative Capabilities and Knowledge Expected for IS Program Graduates". This table included four areas, one of which is technology. Under the technology heading, lists Database Design and Administration and beneath it suggested the topic of "Administration, security, safety, backup, repairs, and replicating" as topic coverage areas.

In addition to the representative capabilities figure, IS2002 included 12 learning unites, each can serve to be a course in traditional IS programs. Security was mentioned as a topic of coverage under two learning units, IS 2002.1 – Fundamentals of Information Systems and IS 2002.2 – Electronic Business Strategy, Architecture and Design.

CC2005

Following IS2002, computer technology field has witnessed a lot of changes that necessitated creating new programs. It also necessitated identifying the domain of each technology field and the areas that overlaps among them. The development of Computing Curriculum 2005 (CC2005) served these two purposes: First, it identified the fields or the academic programs that are supposed to be computer technology programs thus creating different domains of study. Second, it listed specific fields that are included under each domain.

CC2005 identified five computer related programs: Computer Science (CS), Information Systems (IS), Information Technology (IT), Computer Engineering (CE) and Software Engineering (SE). Along with a list of the five technology fields, CC2005 provided a scoring mechanism for the coverage (or domain) area for these five technology fields. Although there is some overlap in the coverage area among these five fields, CC2005 provided ample description of each of the coverage areas for all five.

One of the tables included in CC2005 provides Comparative weight of computing topics across the five kinds of degree programs mentioned above. Two topics were mentioned in this table regarding security: Security issues and principles, and Security implementation and management. The Information Technology domain has the highest score of suggested coverage for both of these topics.

IT2005, IT2008

Both of these are volumes regarding the latest emerging field of information technology. First a draft of this standard curriculum was developed in 2005 and followed by a new volume a couple years later. The information Technology volume received the lion share of coverage regarding information security topics. First it listed Information Assurance and Security as one of twelve coverage area that is listed in the body of knowledge for this field. Second, IT2005 and IT2008 listed information assurance as one of the "Pervasive Themes" that is prominent in the coverage in these areas.

General Observations

Based on the above review of different standard curricula and their inclusion of information security, the following observations can be made regarding the development and progress of information security in standard curriculum:

- Information security is a cross-discipline domain. It is mentioned at various degrees of depth in all the standard curriculums that were noted above. It covers a wide area of technological and non-technological topics, thus it may need to be covered from both perspectives.

- Information security as a topic has been progressing increasingly through the entire curriculum. It started by covering a selective topic in CC2001 to becoming a pervasive theme in IT2005/2008.

- The coverage of information security in academic programs is expected to increase in the future and so does the number of programs that offer it.

PLANNING FOR A NEW PROGRAM

Offering a new program at colleges and universities does not happen haphazardly. Instead, careful planning, considerations and coordination need to be followed in order to assure the success of introducing a new program into academic curriculum. This section discusses the factors that contribute to the success of introducing a new program into academic curricula.

Heinrichs and Banerjee [9] noted four factors that affect the selection of programs and courses within a typical IT/IS program: (1) recommendations of model curricula, (2) skills and technologies desired by employers, (3) the interests of faculty and (4) benchmark studies.

In a study conducted to assess the review of an MIS (Management Information System) program, Yew [15] noted that industry expectations and IT (Information Technology) outlook are the prime factors that shape redesigning or creating new programs.

In another study conducted to evaluate factors that influence the design for technology programs, Slagle and Smith [14] noted:

> "The challenge for a new program is then threefold: identify need (future employer demand), for the program, student interest, and sources of research funds to keep the program running P. 3".

The remainder of this section discusses in more details the factors that influence the selection and components of new programs from four perspectives: faculty interest, market demand, external support and institutional process.

Faculty Interest

Faculty interest is a prime factor that contributes to the success of offering new programs [1]. Faculty members, after all are the individuals who provide the expertise to teach the courses needed in the program. As simple as this may sound, however, a closer look at the interwoven factors of technology programs reveal the placement of more important role of faculty on new programs such as information assurance.

In new programs development, faculty need not only to know the technical aspect of the field, they may also need to learn about future trends for the field as well as pedagogy associated with teaching it. Faculty also may have to suggest new courses and update existing courses. Thus, the stake is high regarding the interest of faculty.

One of the sticking points regarding new evolving programs like information assurance is that the program may not be matured enough to fully identify the domain or the courses to be included [2]. There is no clear benchmark to compare course content of the suggested program because information assurance is new and is continuously evolving.

Market Demand

The market demand is crucial to the success of new programs. Academic programs are known to follow the foot-steps of the market demand. If the demand of the market increases, so does enrollment of specific programs.

Yew [15] used the word "Attractiveness" to refer to the demand on certain programs by students. She noted:

> "Most students consider job prospects a significant factor in their decisions to major in a field of study. Therefore, the student perception of job prospect associated with the degree is expected to be a major factor in determining the "attractiveness" of a program. P. 5".

Institutional Process

Working through the different steps to ensure successful submission of a program within the institution often requires a number of different steps. Introducing a new program often starts by a department submitting a proposal to list the rationale for offering the new program and the courses included in it. From that point, the proposal transcends into the hierarchy through different levels of committees and administrative procedures. Sometimes, these steps and procedures are numerous and require long time to implement. In cases, other departments may object to introducing this new program because it duplicates or overlaps with their programs.

A strategy that has been helpful in the past regarding advancing of new program proposals is to incorporate more than one department in the program. Combining courses from other programs gives more support and stresses the "collaboration" notion that is often encouraged in academic programs. However, such incorporation involves the coordination with the other departments and the continuous inclusion regarding suggested future changes. Thus, a careful balance between the program content and other institutional requirements is needed in determining the number of programs to be included in the proposal as well the course content that are incorporated.

External Support

External support to new programs can come in different formats most notably through accreditation or through grants and additional financial support.

Getting accreditation from a recognized agency is a mean of proving high standards for that department. An accreditation program has long been recognized as a mean of maintaining the highest standards of professionalism [13]. However, educational institutions may place an importance on accreditation for different reasons. For example, the Web Site for ABET, (Accreditation Board for Engineering and Technology), the nationally recognized accrediting organization for engineering and technology curricula at (http://www.abet.org/the_basics.shtml) distinguished institutional accreditation from specialized accreditation as follows:

- **Institutional accreditation** evaluates overall institutional quality. One form of institutional accreditation is regional accreditation of colleges and universities.

- **Specialized accreditation** examines specific programs of study, rather than an institution as a whole. This type of accreditation is granted to specific programs at specific levels.

> Architecture, nursing, law, medicine, and engineering programs are often evaluated through specialized accreditation.

External support may come in the form of funding opportunities. This may cover part of the cost of the program or the entire cost. If funding opportunities are sought for the program, then stipulations on follow up studies and report may be needed. In this case, annual report or follow-up study may be required by granting agency to ensure that the requirements are met regarding funding the program.

INFORMATION ASSURANCE PROGRAM AT IUP

This section elaborates on the experience of the Computer Science (COSC) program at Indiana University of Pennsylvania (IUP) in introducing a new track in Information Assurance. The computer science department offers a Bachelor of Science degree (B.Sc.) in computer science with a track in Information Assurance (IA) since 2001. The development of the program as well as the steps followed went through different course, program and requirement revisions. Thus the experience of this program development is explained here from the four different perspectives that were described in the previous section.

Faculty Interest

Faculty members of the computer science department were interested in introducing the Information Assurance (IA) program. There were many evidences that there is a need for such a program in the curriculum of IUP. However, the contents were not agreed upon initially. Early contacts with other departments, mainly the Criminology Department, helped shape ideas for the courses that need to be offered. The main goal was to use existing resources as much as possible and new courses as needed. The courses from other departments were examined and upon further search, the computer science department decided that they need to add five new courses to the program. Three of these are Computer Science Courses, COSC 316, 356, and 427, Host Computer Security, Network Security, and Cryptography respectively. The other two were Criminology courses, CRIM 321 (Cybersecurity and Loss Prevention) and CRIM 323 (Cybersecurity and the Law).

Upon the inception of this new IA program, several new faculty members have been hired by the department. Although few of them had conducted significant research in security, most felt very enthusiastic about getting involved in the IA program. In fact, some started right away teaching security courses after attending a number of conferences and workshops that polished their security background.

Market Demand

The market demand was high for information security/assurance profession. The market demand for information security/assurance professionals picked up in particular after 9/11 attack and the subsequent concerns that the information stored at various sources is at risk of being exploited and as a result may jeopardize the national security.

The department of computer science was in touch with these developments. They reviewed different sources of data regarding the demand for such professionals and decided to begin researching starting a new program. The administrative procedures took some time to implement but eventually the program has been approved and students stared to get enrolled into that track.

A related issue here was the excellent attendance of the faculty workshops organized by our program to disseminate security awareness in surrounding region and nationwide. More than 40 faculty from various schools across the nation attended the 2001 workshops and about 50 attended in 2002. These figures clearly indicate the interest of faculty in attending such trainings which also reflect market needs to security professionals. Moreover, several of the attendees went back to their home institutions and established security programs that later on were accredited by NSA as CAE-IAE. Our IA program also helped those emerging security initiatives and has established partnerships with several of these institutions.

Institutional Process

The procedures for approving a new program at IUP are long and could take some time before implementing it. The procedures start by a proposal from a committee at the department level, to another committee at the college level. After that, a university wide curriculum committee has to approve the new program. Subsequently, the new program has been approved by the IUP Senate and then was forwarded to the State System of Higher Education (SSHE) which also approved its launching.

Realizing these steps, the computer science department did two things: first, it formed a university wide committee that oversees the development of this new program. This committee was widely represented, it include individuals from all colleges of the university. Second, it formed an alliance with the criminology department so to include courses from both programs in this new degree program.

Accreditation and External Support

The computer science department sought to be designated by the National Security Agency (NSA) as a Center of Academic Excellence in Information Assurance Education (CAE-IAE). It was realized from the beginning that getting this support from NSA will serve two purposes: first, it provides some funding for the program thus helps with the start and continuity of the program. Second, it provides broader recognition for the program and thus adds to the “attractiveness” of the program.

In most countries in the world, the function of educational accreditation is conducted by a government organization, such as a ministry of education. In the United States, however, the quality assurance process is independent of government and performed by private membership associations [1].

The development efforts for the above-mentioned new courses were supported by a number of capacity building grants from National Science Foundation (NFS), DoD, Cisco and NSA. These external supports also helped several faculty members through release time to start a number of security related research initiatives in order to strengthen this emerging program.

SUMMARY AND FUTURE RESEARCH

This paper explained about the development of an information assurance program at a higher education institution. It focused on the experience of the computer science department at Indiana University of Pennsylvania and their Bachelor of Science degree program in computer science - Information Assurance track. The paper began by giving a review of the literature regarding information assurance. It provided definitions and gave a brief history on the use of such term. Then the paper focused on the use of such term in academia and shifted the focus more on the B.Sc. degree offered at Indiana University of Pennsylvania. It gave details on how this program started and how they implemented the courses.

While writing this paper and due to time constraints, a lot of details have been compromised. In many instances some examples could be presented to further illustrate what was discussed in each section. For example, a much more in-depth discussion of the coverage of information assurance in various standard curricula could shed more light on information security from this perspective. Also, listing some examples of professional organizations in information security, their goals and formation may help the reader to identify the issues that these organizations deal with. So once again, we feel that some details were compromised in the paper. Thus the intention of the authors of this paper is write a second paper that gives more in-depth information about various programs that offer information security in their curricula. The intended paper will focus also on different standard curricula (CC2005, IT2005, IT2008 and CC2005). It will list also the different organizations in these fields, the disposition of such programs and the latest development regarding the selection of courses in such programs.

REFERENCES

1. Bacon, T., Tikekar, r. Experiences with developing a computer security information assurance curriculum. Journal of Computing Sciences in Colleges, 18(4), 254-267. Retrieved November 17, 2008 from ACM digital library http://www.acm.org/dl.
2. Bogolea, B., Wijekumar, K. (2004). Information security curriculum development. Proceedings of the 1st annual conference on Information security curriculum development 59-65.
3. Chen, K. (2003). A Web Security System Model. Issues in Information Systems Vol. IV (2) 404-415.
4. Computing Curricula 2001: Computer Science: Report of The Joint Task Force on Computing Curricula, IEEE Computer Society and The Association for Computing Machinery, December, 2001. http://www.acm.org/education/curricula.html.
5. Computing curricula 2005 the overview report (2005). Retrieved October 2, 2006 from ACM Digital Library http://www.acm.org/dl
6. Computing Curricula Information Technology Volume (2005). Retrieved March 4, 2007 from ACM Digital Library http://www.sigite.org/.
7. Computing Curricula Information Technology Volume (2008). Retrieved February 8, 2009 from http://www.acm.org/education/curricula.html.
8. Dennis, T., El-Gayar, O., Streff, K. (2004). A Model Program in Information Assurance and Computer Security. Issues in Information Systems Vol. V, No 1. 97-102.
9. Heinrichs, L.; Banerjee, D. (2002). In Search of The Typical IS Program. Issues in Information Systems, III, 243-249
10. Innella, P. (2008). *A Brief History of Network Security and the Need for Adherence to the Software Process Model.* Retrieved December 10, 2008 from http://www.tdisecurity.com/resources/assets/NetSec.pdf
11. IS 2002: Model Curriculum and Guidelines for Undergraduate Degree Programs in Information Systems. (2002). Association of Information Technology Professionals, Retrieved October 4, 2006 from http://www.acm.org/education/curricula.html
12. Leeuw, K. D., Bergstra, J. (2007). *The History of Information Security: A Comprehensive Handbook.* New York, NY: Elsevier
13. New Jersey State Association of Chiefs of Police (2002). New Jersey Association Law Enforcement Program. Retrieved March 1, 2009 from http://www.gtpd.org/Accred%20overview.pdf.
14. Slagle, J. M.; Smith, D. A. Designing a New Program for ABET Accreditation. *Proceedings of the 2008 ASEE North Central Section Conference,* 1-8. Retrieved March 20, 2009 from http://www.asee-nc.org/Conferences/
15. Yew, Bee K. (2008). A Perspective on a Management Information Systems (MIS) Program Review. *Journal of Information Technology Education, 7, 299-314.*