NSA Centers of Excellence in Information Assurance Education and the Certified Information Systems Security Professional Domains: How Do They Compare?

Albert Fundaburk
afundabr@bloomu.edu
Business Education/Office Information Systems
Bloomsburg University
Bloomsburg, PA 17815 USA

Abstract

This research collected data from 321 faculty members from universities designated as National Security Agency Centers of Academic Excellence in Information Assurance Education to determine the extent these universities are teaching the areas identified in the 10 domains of the Certified Information Systems Security Professional examination. This question was answered by a researcher developed survey which was confirmed valid using a panel of 18 Certified Information Systems Security Professionals and reliable using Cronbach's Alpha and Split-Halves reliability. The findings of this research indicate that the areas identified in the 10 Domains of the Certified Information Systems Security Professional examination are being taught from a high of between often and always to a low of between sometimes and rarely.

Keywords: Info Sec Education, Information Security Curriculum, Information Security, NSA Centers of Excellence, Information Security Skills

1. INTRODUCTION

The Internet has allowed a world so interconnected that work cannot be accomplished without computers, and computers cannot perform effectively without a measure of security. Due to the shortage of information systems security professionals a need exists for a comprehensive program to educate more individuals in the field of Information security (Chin, Irvine, & Frincke, 1997). To meet this need The National Security Agency (NSA) developed its Centers of Excellence in Information Assurance Education to encourage universities to develop information security curriculum. To be awarded the National Security Agency's Centers of Academic Excellence in Information Assurance Education, schools must have curriculum mapped to National Security Telecommunications and Information Security Committee (NSTISSC) *4011 National Training Standard for Information Systems Security (INFOSEC) Professionals*, an eight year old document (Centers of Academic Excellence in Information Assurance Education, 2002). However, the NSTISSC focus was to provide standards for practical vocational skills. Mainstream colleges and universities have goals that may or may not be compatible with those of the standards dictated by NSTISSC (Yasinsac, 1999).

Information security as a field has not matured sufficiently to develop processes associated with performing specific information security tasks. Until these tasks are identified and related standards produced, effective standardized information security curricula can not be developed (Reynolds, 1998). Due to this lack of standardization many organizations have implemented professional certification programs. Although professional certifications in information security are said to be based on a common body of knowledge, there is still a fundamental difference of opinion as to what constitutes this common body of knowledge. Many practitioners of information security feel that to further define information security and to legitimize its existence there should be accredited college curricula (Saita, 2002).

The International Information Systems Security Certificate Consortium (ISC)[2] was instrumental in the development of the Certified Information Systems Security Professional (CISSP), the most comprehensive certification for information systems security professionals (Dugan & Prencipe, 2001). Although CISSP was not the only certification available for information systems security professionals, it was the only broad top-down certification covering theoretical knowledge of 10 domains recognized to be required for information security certification and for many organizations the CISSP was considered to be the gold standard in information security (Dugan & Prencipe, 2001). It was this theoretical knowledge that needed to be the baseline for identifying skills for a common body of knowledge in information security. This baseline was used to evaluate whether NSA Centers of Excellence in Information Assurance Education were providing the appropriate education for information security professionals.

This research examined the 10 CISSP domains from within the information systems security work environment to determine which skills were deemed necessary and then surveyed existing NSA Centers of Academic Excellence in Information Assurance Education faculty to determine which skills from within the 10 domains were being taught. Using empirical methods the goal of this research was to determine if existing curriculum in colleges and universities designated as NSA Centers of Academic Excellence in Information Assurance Education was consistent with the needs of an information systems security work environment.

2. REVIEW OF LITERATURE

Several steps were used for the purpose of reviewing existing literature and research. Initially, the following databases were used: ACM Digital Library, Applied Science and Technology, Computer Abstracts, Computer and Information Systems Abstracts, ProQuest, and EBSCOhost. The searches were conducted by focusing on keywords used in each of the databases. The keywords used were: information technology (IT), infosec, information security, information security education, computer security, computer security curriculum, information systems curriculum, CISSP, information systems security certification and information systems security requirements. The second step required reviewing all documents, journals, texts, and books, identified using these keywords, for applicability to the research.

The review of literature revealed limited research on the actual tasks required for success as an information systems security professional. Although numerous articles discussed information security curriculum, very few were empirical in nature, nor rigorous in the research used in developing the curriculum.

Carnegie Mellon University supported the contention that there is no set of skills identified as being necessary in information security curriculum development:

> There apparently is no systematic agreement on the knowledge, skills, and abilities required to formulate a curriculum for information assurance and security professionals that enjoys a broad-based support across organizations ("Information Assurance Curriculum", 1999).

The International Information Systems Security Certificate Consortium (ISC^2) model attempted to standardize information security into a Common Body of Knowledge (CBK) (Logan, 2002). This organization's CISSP examination was developed to ensure that information systems security professionals met standard criteria of knowledge and continued to upgrade that knowledge (Krutz & Vines, 2001).

The University of Maryland recognized the CISSP as being instrumental in identifying a common body of knowledge for implementation in its business management curriculum. Although Hazari (2002) admitted that it did not provide sufficient course work in finance, organization or strategy, it did lay the ground for basic information security.

Kim and Choi (2002) came close to identifying the work actually performed by information systems security professionals in the field. Their research on identifying the educational requirements for information systems security professionals in Korea identified the following as essential for practitioners of information security. In order of importance they were:

1) establishing information security policy
2) establishing managerial security measures
3) analyzing security environments
4) risk analysis and assessment
5) understanding basic cryptology
6) acknowledging laws and regulations
7) testing vulnerabilities in information security systems
8) designing physical security measures
9) coping with hacking
10) managing intrusion check and detection
11) privacy and ethics
12) handling computer viruses
13) knowledge of information security standards
14) managing security education programs
15) knowledge of security system evaluation (Kim and Choi, 2002).

The determination of key educational requirements for information systems security professionals by security experts was an important contribution to the improvement of information security program development (Kim and Choi, 2002). Kim and Choi's (2002) study gave impetus to the need for more rigorous and empirical research in defining the skills and attributes of information system security professionals in the field.

3. METHODOLOGY

This research performed a rigorous review of the teaching of information systems security skills and provided an answer to the following question: Are universities designated as NSA Centers of Academic Excellence in Information Assurance Education teaching the skills identified in the CISSP examination?

This question was answered by a survey of existing NSA Centers of Academic Excellence in Information Assurance Education faculty to determine which skills from within the 10 domains of the CISSP were being taught. Using empirical methods the goal of this research was to determine if existing curriculum in colleges and universities designated as NSA Centers of Academic Excellence in Information Assurance Education was consistent with the needs of an information systems security work environment as defined by the CISSP.

Data collection was accomplished by using sampling survey research. In the design of this research two issues were addressed:

1) identifying a sufficient sample size, and
2) instrument reliability and validity.

In their article on determining sample size Bartlett, Kotrlik, and Higgins (2001) included a table for determining minimum required sample sizes based on mathematical formulas, which used a margin of error of .03, an alpha of .05, and a t of 1.96. There were 323 faculty members in the target population. Bartlett, et al. (2001) identified 85 responses as being representative of a population numbering 300. To ensure an adequate sample size, all 323 respondents were surveyed.

The survey consisted of 23 questions developed from the following CISSP domains: 1) Access Control Systems and Methodology, 2) Telecommunications and Network Security, 3) Security Management Practices, 4) Applications and Systems Development Security, 5) Cryptography, 6) Security Architecture and Models, 7) Operations Security, 8) Business Continuity Planning and Disaster Recovery Planning, 9) Laws, Investigations, and Ethics, and 10) Physical Security (CISSP Certification, 2000). These questions used a five point verbal frequency scale as follows: 1) always, 2) often, 3) sometimes, 4) rarely, and 5) never. The following points were assigned to the scale to facilitate statistical analysis: always (5 points), often (4 points), sometimes (3 points), rarely (2 points), and never (1 point).

The pilot survey was analyzed to identify errors in form or presentation, or identify shortcomings within the questions. The survey was changed to address these issues and then re-administered to the pilot survey committee for additional comments. Upon finishing the survey, the committee members were interviewed individually to ascertain their reaction and comments. As a result of the pilot survey minor changes in format and content were made.

Validity was evaluated by using a panel of 18 experts, drawn randomly from the population of information systems security professionals, who were considered to have knowledge and/or skills in information security by virtue of their CISSP certification.

This research used a modified Delphi technique to assess the content validity of the survey. The modified Delphi approach consisted of identifying a select group of information systems security professionals who, by successive rounds, collaborated on the development of a survey to identify specific competencies, taken from the CISSP examination, which should be taught in an academic environment.

In the reliability phase the survey was distributed to a random sample of the population and tested for split-half reliability. The instrument was deemed to be reliable based on the split-halves method. Using Statistical Program for the Social Sciences (SPSS) to perform the split-halves computation the following results were noted: Guttman split-half =.8572, unequal-length Spearman-Brown = .8614.

Table 1, Split-halves Results for Reliability Phase

Reliability Coefficients	
N of Cases = 26	N of Items = 23
Correlation between forms = .7562	Equal-length Spearman-Brown = .8612
Guttman split-half = .8572	Unequal-length Spearman-Brown = .8614
12 Items in part 1	11 Items in part 2
Alpha for part 1 = .8334	Alpha for part 2 = .8719

To confirm the split-halves reliability, a computation of Cronbach's was performed. The standardized alpha for the 23 question scale was 0.9141, indicating a high degree of internal consistency with all items exhibiting a positive Corrected Item-Total Correlation. Because deleting any item would have no significant effect on the overall scale reliability, all 23 items were justified for retention.

Table 2, Cronbach's Alpha
Reliability Analysis

Reliability Coefficients

N of Cases = 26.0
N of Items = 23

Alpha = .9141

The survey was made available on a secure Web server using forms developed using Microsoft FrontPage®. The responses from these forms were sent to a database on the Web server with separate tables for each of two response areas: 1) information systems security faculty validation, and 2) information systems security faculty surveys. Responses were tracked using randomly assigned Personal Identification Numbers (PINs). At the conclusion of data collection all references relating PINs to e-mail addresses were deleted in compliance with Bloomsburg University's Institutional Review Board (IRB) requirements.

From the sample of 321 (N) information systems security faculty the total 321 (n) were used with a survey response rate of 31%. The database results were exported to an Excel spreadsheet. The raw spreadsheet data was then migrated to SPSS for analysis.

4. RESULTS

The results of this survey indicate that, for the most part, NSA Centers of Excellence in Information Assurance Education are teaching in the information security areas identified by the CISSP. The teaching area receiving the most interest was Edu20, computer crime, which was taught from often to always. The teaching area receiving the least interest was Edu6, implementation and management of change control, which was taught from rarely to sometimes (see Appendix 1).

The following teaching areas, from highest to lowest, were taught often: edu11, cryptographic concepts, methodologies and practices, private and public key algorithms, and public key infrastructure; Edu7, the development or implementation of information security employment policies, practices, standards, guidelines, and procedures; Edu13, principles of common computer and network organizations, principles of common security models, and evaluation techniques; Edu5, communications and network security, Internet / Intranet / Extranet, e-mail security, facsimile security, secure voice communications, and security boundaries; Edu17, monitoring tools and techniques, intrusion detection and penetration detection techniques, threats and counter measures; Edu14, common flaws and security issues associated with systems architecture and design; Edu2, identification and authentication techniques; and Edu8, security awareness training and management (see Appendix 1).

The following teaching areas, from highest to lowest, were taught between sometimes and often: Edu3, intrusion detection monitoring, and penetration testing; Edu1, access control techniques, access control administration, and access control models; Edu19, procedures for emergency response, extended back-up and post-disaster recovery; Edu4, International Standards Organization/Open Systems Interconnection, Layers and characteristics; Edu9, information security involving database and data warehousing, and information storage; Edu23, concepts of protection from physical security threats; Edu22, concepts of computer ethics; and Edu21, information security incident handling and investigations (see Appendix 1).

The following teaching areas, from highest to lowest, were taught sometimes: Edu16, administrative management concepts, resource protection, audit trails, inappropriate activities, violations, breaches, and reporting; Edu18, protection of critical business processes; Edu10, information security regarding knowledge based systems and development controls; Edu15, systems architecture evaluation techniques; and Edu12, system architecture for implementing cryptographic functions (see Appendix 1).

5. SUMMARY

This research performed a rigorous review of the teaching of information systems security skills in NSA Centers of Excellence in Information Assurance Education and provided an answer to the following question: Are universities designated as NSA Centers of Academic Excellence in Information Assurance Education teaching in the 10 domains of information security identified in the CISSP examination? This question was answered by a survey of existing NSA Centers of Academic Excellence in Information Assurance Education faculty to determine which skills from within the 10 domains of the CISSP were being taught. The validity of the survey was determined by a panel of experts using a modified Delphi technique. The reliability of the survey was determined by the split-halves statistical measure and confirmed by Cronbach's Alpha. The resulting data from the survey was analyzed using descriptive statistics. The findings of this research indicate that, for the most part, NSA Centers of Excellence in Information Assurance are teaching in the information security domains identified by the CISSP examination. Regarding the skills best identified as being necessary in an information systems security curriculum, the following three questions are indicated for further research:

1. How should existing information systems security curriculum be changed to better meet the needs of information systems security professionals working in the field?

2. Should broad principles or specific applications relating to the skills and attributes identified in an information systems security work environment be taught?

3. Is there a correlation between what is being taught and what is being performed in the field?

It should be emphasized that this research was designed to evaluate the skills and attributes relating to the CISSP certification and existing curriculum in institutions designated as Centers of Academic Excellence in Information Assurance Education. It did not look at any of the many ongoing information systems security programs at schools not so recognized by NSA, nor did it consider any of the skills and attributes identified by any of the other information systems security certifications available. As such, the results from this research should be kept in the context of an evaluation of the skills and attributes identified only in the CISSP and confined to the curriculum in NSA designated Centers of Academic Excellence in Information Assurance Education. The results of this study can be used as a baseline to develop information systems security curriculum. However, further research is needed to determine the correlation of the teaching areas identified with what is being done in the field.

REFERENCES

Bartlett, J. E., Kotrlik, J. W., & Higgins, C. C. 2001. "Organizational research: Determining appropriate sample size in survey research". Information Technology, Learning, and Performance Journal, 19, pp. 43-50.

Centers of Academic Excellence in Information Assurance Education. Retrieved December 2, 2002 from http://www.nsa.gov/isso/programs/coeiae/measure.html

Chin, S., Irvine, C., &. Frincke, D. 1997. "An information security education initiative for engineering and computer science". Paper presented at Syracuse University, Syracuse, NY.

CISSP Certification Common Body of Knowledge Study Guide 2000. Available from The International Information Systems Security Certification Consortium, Shrewsbury, MA.

Dugan, S. & Prencipe, L. W. (2001). "Certifiability secured". InfoWorld, 23, 36.

Golshani, F., Panchanathan, S., Friesen, O., Park, Y. C. & Song, J. J. 2001. "A comprehensive curriculum for IT education and workforce development: An engineering approach". Proceedings of the Thirty Second SIGCSE Technical Symposium on Computing, February, pp.238

Hazari, S. (2002). "Reengineering an information security course for business management focus". Journal of Information Systems Education, 13, pp 23.

"Information assurance curriculum and certification: State of the practice" (1999) Retrieved August 2002 from http:www.sei.edu/publications/documents/99.reports.

Kim, S. & Choi, M. (2002). "Educational requirement analysis for information security professionals in Korea". Journal of Information Systems Education, 13, pp. 237.

Krutz, R. L. & Vines, R. (2001). The CISSP Prep Guide. New York: Wiley.

Logan, P. Y. (2002). "Creating an undergraduate information security emphasis within information technology". Journal of Information Systems Education, 13, pp. 177-182.

Reynolds, W. (1998). "Report of the 1998 Annual Meeting for the National Colloquium for Information Systems Security Education". Retrieved, December 2002, from http:// www.jmu.edu.

Saita, A. (2002). "Bridging the gap". Information Security, 5, pp. 38.

Yasinsac, A. (1999). "Information security curricula in computer science department: Theory and practice", Florida State University. Unpublished manuscript, Florida State University, Tallahassee, FL.

Appendix 1: Teaching areas sorted by frequency taught

Teaching Areas	Means <u>M</u>	Frequency Taught
Computer crime	4.303	Between often and always
Cryptographic concepts, methodologies and practices, private and public key algorithms, and public key infrastructure	4.0808	Often
Development or implementation of information security employment policies, practices, standards, guidelines, and procedures	4.0303	Often
Common computer and network organizations, principles of common security models, and evaluation techniques	3.9798	Often
Security controls when addressing communications and network security, Internet / Intranet / Extranet, e-mail security, facsimile security, secure voice communications, and security boundaries	3.9596	Often
Monitoring tools and techniques, intrusion detection and penetration detection techniques, threats and counter measures	3.9495	Often
Common flaws and security issues associated with systems architecture and design	3.9091	Often
Identification and authentication techniques	3.899	Often
Security awareness training and management	3.889	Often
Intrusion detection monitoring and penetration testing	3.7576	Between sometimes and often
Access control techniques, access control administration, and access control models	3.7172	Between sometimes and often
Procedures for emergency response, extended back-up and post-disaster recovery	3.697	Between sometimes and often
International Standards Organization/Open Systems Interconnection, layers and characteristics	3.6768	Between sometimes and often
Information security involving database and data warehousing, and information storage	3.6768	Between sometimes and often
Concepts of protection from physical security threats	3.6768	Between sometimes and often
Concepts of computer ethics	3.5556	Between sometimes and often
Information security incident handling and investigations	3.444	Between sometimes and often
Administrative management concepts, resource protection, audit trails, inappropriate activities, violations, breaches, and reporting	3.4343	Sometimes

Critical business processes	3.3838	Sometimes
Information security regarding knowledge based systems and development controls	3.222	Sometimes
Systems architecture evaluation techniques	3.1313	Sometimes
System architecture for implementing cryptographic functions	3.0505	Sometimes
Implementation and management of change control	2.7778	Between sometimes and rarely