Scientific Research Publishing

Journal of Information Security, 2020, 11, 177-188
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Empirical Evidence for a Descriptive Model of Principles of Information Security Course

Adeyemi A. Adekoya[1], Aurelia M. Donald[1], Somasheker Akkaladevi[1], Akinjide A. Akinola[2]

[1]Virginia State University, Petersburg, VA, USA
[2]University of Lagos, Lagos, Nigeria
Email: aadekoya@vsu.edu, adonald@vsu.edu, sakkaladevi@vsu.edu, aakinola@unilag.ng.edu

How to cite this paper: Adekoya, A.A., Donald, A.M., Akkaladevi, S. and Akinola, A.A. (2020) Empirical Evidence for a Descriptive Model of Principles of Information Security Course. *Journal of Information Security*, **11**, 177-188.
https://doi.org/10.4236/jis.2020.114012

Received: June 13, 2020
Accepted: August 18, 2020
Published: August 21, 2020

Abstract

The purpose of this study is to examine the nature and content of the rapidly evolving undergraduate Principles of Information/Cybersecurity course which has been attracting an ever-growing attention in the computing discipline, for the past decade. More specifically, it is to provide an impetus for the design of standardized principles of Information/Cybersecurity course. To achieve this, a survey of colleges and universities that offer the course was conducted. Several schools of engineering and business, in universities and colleges across several countries were surveyed to generate necessary data. Effort was made to direct the questionnaire only to Computer Information System (CIS), Computer Science (CS), Management Information System (MIS), Information System (IS) and other computer-related departments. The study instrument consisted of two main parts: one part addressed the institutional demographic information, while the other focused on the relevant elements of the course. There are sixty-two (62) questionnaire items covering areas such as demographics, perception of the course, course content and coverage, teaching preferences, method of delivery and course technology deployed, assigned textbooks and associated resources, learner support, course assessments, as well as the licensure-based certifications. Several themes emerged from the data analysis: (a) the principles course is an integral part of most cybersecurity programs; (b) majority of the courses examined, stress both strong technical and hands-on skills; (c) encourage vendor-neutral certifications as a course exit characteristic; and (d) an end-of-course class project, remains a standard requirement for successful course completion. Overall, the study makes it clear that cybersecurity is a multilateral discipline, and refuses to be confined by context and content. It is envisaged that the results of this study would turn out to be instructive for all practical purposes. We expect it to be one of the most definitive descriptive models of such a cardinal course, and help to guide and actually, shape the decisions of universities and academic

programs focusing on information/cyber security in the updating and upgrading their curricula, most especially, the foundational principles course in light of new findings that are herein articulated.

Keywords

Benchmark, Cybersecurity, Descriptive Model, Survey results, Certifications, Common-Body-of-Knowledge, Empirical Evidence, Principles of Information/Cybersecurity Course, Tools Deployed

1. Introduction

Offering Cybersecurity courses in colleges and universities across the globe has become an increasingly popular phenomenon and trend in the last decade. Uncountable Colleges and Universities have joined the bandwagon of offering and teaching Cybersecurity courses. This shift in curriculum has become the cynosure of the computing discipline redesign in this day and age [1]. A synoptic review of a typical, and contemporary Information security Principles course appears to have been designed to address widely varied and divergent cybersecurity topics and issues. In fact, a cursory inspection of a sample of the courses' syllabi shows that the course content and coverage vary as widely as the departments in which the courses are taught. It is safe to assert that there is neither rhyme nor rhythm as to what is taught and how the course is taught at this time. The need for the standardization of the course cannot therefore, be overemphasized, and such a need led to this study. Elements of the benchmark for the Principles of Cybersecurity course, as far as we know, have not been properly established. In fact, Schneider [2] and Santos [3] show that there are no benchmarks for much of Information Security courses, and the Principles of Information/Cybersecurity is not an exception. Although there is substantial curriculum-based MIS/CS research in the discipline, pedagogical research in Cybersecurity is relatively sparse. As a modest start and within recent years, some of the institutions represented in the study sample have moved towards standardizing their course offering through the establishment of the Principles of Cybersecurity course in accordance with the requirements of vendor-based and other vendor-neutral certification dictates. Also, within recent years, various computing and related programs are moving towards standardizing these courses in accordance with individual regular college—accreditation and program—certification requirements. There have been concerted efforts by course instructors to cover as much as possible of contemporary cybersecurity topics. For the most part, they focus on cybersecurity foundations, risks analysis and management—identification, assessment and control, cryptography, human aspects of cybersecurity to include policy, education, training and awareness—incidence response, disaster recovery, business continuity. Other areas include Virtual Private Networks (VPNs), Intrusion Detection and Prevention Systems and more specific topics such as

defense by obscurity, perimeter defense, and defense-in-depth, Policy, Law, and Ethics are not excluded from course coverage.

This study investigated the structure of Principles of Information Security courses with a view of identifying commonalities and overlaps in course content and as well as the inherent variance. Questions that are germane and addressed include whether there currently exists a benchmark Principles of Information Security course and what constitutes the primary intellectual substance of such a course? Other questions are: 1) Is there a benchmark Principles of Cybersecurity course? 2) What is the intellectual substance of such a course? 3) How have theory and laboratory work been integrated into the course to present a logical whole? By identifying a common core and overlaps of the subject matter, we hope to have provided a basis for streamlining the process that could serve as a vehicle for the eventual standardization of the course. More specifically, the purpose of the study which is many and varied, primarily are: to help fulfill the need for the establishment of benchmarks and standards for the Principles of Cybersecurity course, to fill the cybersecurity curriculum content deficit, and to achieve the need for the establishment of benchmarks and standards of Principles of Information Security course.

For background, this research draws from published works in the area of standardizing curricula and course content in the Cybersecurity domain which so far, and as pointed out by Fischer [4] has been sparse. However, there are few known reported studies in the information/cybersecurity extant literature that have dealt with relevant curriculum questions. Even among the published works, much focus has been directed at non-content aspects, course outcomes and exit course requirements expected of students. More pointedly, Schneider [2] remarked that "an educated computer security workforce is essential for building trustworthy systems. Yet, issues about what should be taught and how, are being ignored by many of the University faculty who teach cybersecurity courses—a problematic situation." Nonetheless, as part of an evolving science that draws on the established framework and published research, the study still builds upon the scanty literature that exists.

Moreover, for a relatively long time now, researchers such as Fischer [4], Alli *et al.* [5], and Ayoub [6] have expressed their dissatisfaction and indeed, a concern for a lack of content convergence and cumulative tradition of the field's subject matter. It has also been recognized that the discipline does presently lack cohesion in the Common-Body-of-Knowledge (CBK), driving the foundational courses in Information Security [6] [7] [8].

No doubt, the rise in cyber security infringements has led to the need for a sound cyber security curricula. A well-thought-out cyber security curriculum insures that students are equipped with a firm foundation of the field and are trained in the state-of-the-art techniques needed to analyze, design and actually implement secure technology infrastructures as pointed out by both Bogolea and Wijekumar [9], and Whitman and Mattord [10].

In addition, Whitman and Mattford [10], noted the up-trending statistics on

security infringements which have stimulated faculty, researchers and students' growing interest and direct involvement in cyber security. This development has ultimately, promoted the burgeoning and timely growth in the cyber professionals' pool. That same need for the training and development of more cyber security professionals was recognized and alluded to by Theoharidou, and Gritazalis [11] leading to the argument for, and the determination of a CBK needed to develop a long overdue, standard cyber security curriculum.

Numerous other prior literature addressed the lack of guidelines for designing and implementing information systems security curricula [9] [10] [12] [13] [14]. The call to remedy the deficit resulted in several proposed education models and much improved curricula [2] [6] [7] [8] [15] [16] [17]. It must be pointed out that the expressed concern is yet to be remedied, while universities are still grappling with the need to provide students with the cognate skills needed by employers. It is also interesting to note that Luallen and Labruyere [16] recommended among others, that a sound cybersecurity curriculum should consist of testbed projects coupled with rapid prototyping in order to provide students with hands-on, learn-by-doing class experience. Ultimately, the ever-present challenge as noted much earlier by Chin, Irvine, & Frincke [12], is the need to train students and individuals that can analyze, design, develop, and deploy complex and trusted cybersecurity systems with confidence.

It is also worth mentioning the numerous studies, reports and white papers that treat cybersecurity academic preparation and industry-readiness of students [18] [19] [20]. These reports individually and collectively, factor into the literature base and the conceptual framework guiding the study. More specifically, this study aims at gathering and reporting empirical data and evidence to support future design of standardized principles of information security course.

2. Methodology

To lay the foundation for the design of a standardized undergraduate-level Principles of Information/Cybersecurity course, a survey of universities and junior colleges was conducted. The research principle was couched in 1) a sample survey—which emphasizes statistical inference; and 2) personal interviews which emphasize qualitative data.

The study gathered empirical data to determine benchmarks, commonalities and overlaps in content knowledge, skills and abilities covered by the typical Principles of Information Security Course. The survey was made available to purposive sample departments such as CIS, CS, MIS, Engineering and IS-related programs with prior knowledge that they offer cybersecurity or semblance courses. The list of programs was fairly exhaustive and up-to-date. To guarantee a reasonable participation rate, no attempt was made to generate a random sample from the directory. The list in effect, served as the population frame. A questionnaire was posted on Virginia State University's Qualtrics link. The questionnaire was also shared with other respondents through e-mail as well as regu-

lar mail to contact-persons at each of the institutions. The sample size consists of 187 colleges and universities.

2.1. Research Plan

The research plan consists of a Research Procedure, and the process of obtaining research data. Figure 1 and Figure 2 illustrate the research steps and the sample data breakdown.

The research data derived from 187 Universities and Colleges, 87% of which were Universities and 13% of which were 2-year junior colleges.

Figure 2 shows a breakdown of the research sample by university and 2-year college categories.

2.2. Instrument and Data Sources

The primary instrument deployed was an omnibus instrument consisting of many parts ranging from demographics, through the different aspects of the survey germane to the relevant course attributes being investigated; it is a 62-question

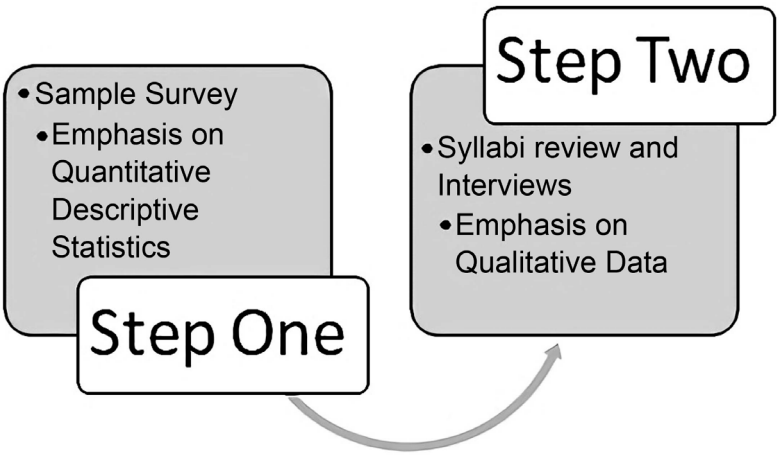

Figure 1. Research plan.

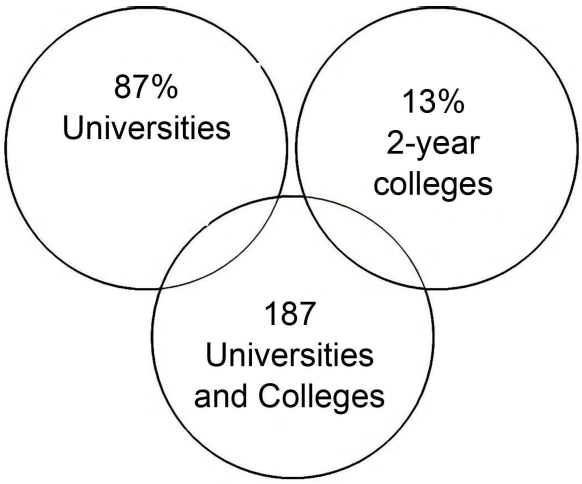

Figure 2. Sources of sample data.

survey covering respondent's perception of course, content, coverage and method of delivery including open-ended, Likert-scale, and multiple-selection types. Some of the questions focused on level of emphasis of different areas of cybersecurity course, activities and certification-bias, and were measured using a five-point Likert scale while others specifically focused on identifying commonalities among the different aspects of the course. Also, the survey was sent through a variety of outlets including cybersecurity-related programs faculty listing, and other channels such as e-mails, regular mails and personal contacts, to designated persons at each of the institutions particularly, in developing countries. We received 94 complete, usable questionnaires representing a 50.2% return rate. These questionnaires were deemed valid, and used in the final analysis.

3. Data Analysis

3.1. Emerging Paradigms for the Course

Descriptive and inferential statistics characterized by simple frequency counts, and percentage breakdowns were carried out. There are certain paradigms, which a priori, were expected to provide context for our definition of the Principles of Information Security course. As speculated, and from a preliminary review of the survey results, four (4) main themes emerged.

Additionally, several course syllabi were solicited, and reviewed for their structure, layout, course coverage and their CBK-focus. The emerging themes are depicted in a 4 interlocking circles shown in Figure 3. The thematic composition of the average Principles of Information Security course based on the gathered data are: the sociotechnical nature of the typical course constituted primarily by Technology, Human factors, Rick Management, Policy, Law and Ethics. The distribution of and coverage of focus by area in all probability, varies widely. It must be pointed out, however, that depending on the academic-bias of the department

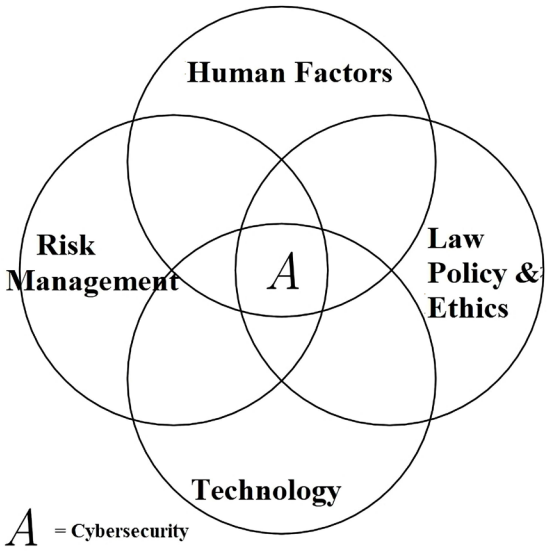

Figure 3. Elements of principles of cybersecurity course.

that offers the course, some departments emphasized technology over human factors and vice-versa.

As to be expected, different programs placed varying degrees of emphasis on the contributing elements and their externalities, which are deemed adjunct to the core cybersecurity subject matter. Also, the trailing list highlights some of the emanating attributes of the course, *i.e.*

1) The Principles of Information Security course is an integral part of most information/cybersecurity programs.

2) Most Principles of Information Security, courses stress both strong technical and strong organizational skills.

3) Most Principles of Information Security, courses encourage students to study beyond the classroom, for certifications, and to consider licensure options.

4) Course instructions continue to be dominated by instructor-led lecture method, although small group exercises, individual projects and presentations are often included.

3.2. Quantitative Descriptive Analysis and Results—Cybersecurity content

On the content side, some analyses suggest that Principles of Information System course seem to be most similar, however, on the substance and depth of course coverage.

Oddly enough, there exists much variance on the substance and depth of coverage. The home-college of the program—Engineering/Business dichotomy seems to factor into the course emphasis. Against that backdrop, the challenge of Principles of Information Security not being a uniform course remains a pedagogical limiting factor; this effort seems to have opened the door for an effective remedy.

The following statistics were derived from the survey:

1) The 50.2% return rate of the survey responses indicates respondents' institutional descriptions namely: 7% exclusively 2-year colleges; 68% exclusively 4-year colleges; 15% both undergraduate and graduate programs, and 10% exclusively graduate programs.

2) As to the department where the course is taught, data revealed that the Principles of Information Security is taught across very few academic units and departments; Computer Science, and Computer Information Systems turn out to be the most representative suggesting the limitation of its academic landscape and footprints.

3) 54% of the institutions have full-fledged information/cyber security major or minor amongst their programs.

4) 72% of respondents reported to have an established Information security curriculum established in their institutions.

5) Majority of the programs have the curriculum follow a sequence of the Introduction/Advanced-level courses format.

6) Course titles vary widely; however, "Principle" remains a critical keyword

in a greater percentage.

7) The analysis corroborated the long-held thesis in the field that basic standards in course coverage and other aspects of course design are non-existent, and in some cases, are under construction.

8) The structure and content of the Principles of Information Security course is diverse and divergent as it could get. The major commonalities include—Technology, Risk Management, Policy, Law and Ethics, and Human Factors. Moreover, the sociotechnical perspective of Cybersecurity shines through.

9) The data on the course coverage reveal a sharp contrast between the human and the technology emphases. While the human aspects address Policy, Education, Training and Awareness issues, the Technology element for the most part, treats Redundancy, Intrusion Detection and Protection Systems (IDPSs), Confidential services and Implements (*i.e.*, PKI, cryptographic communications, etc.), as well as elements of Digital Forensics, Vulnerability and Risk Assessment.

10) The mode of teaching is for the most part, a blend of classroom-based sit-in instruction, pure-online virtual learning, and a variety of click-and-mortar types of instruction delivery.

11) Open-ended questions which encouraged spontaneous and unstructured responses were instructive. Not only did they shed light on the larger question of what improvements could be introduced, it further drew out respondents' opinions, attitudes or suggestions. Ultimately, there was a unanimous recommendation that much time and effort should be devoted to the practical, hands-on aspect of the course. Also, focusing on vendor-neutral certifications was not left out of account.

12) Tools deployed to teach the course can be divided into two major categories: hardware and software. They are generally Graphical User Interface tools designed to perform cybersecurity functions. It is noteworthy that certain Intrusion Detection and Penetration Testing Tools that are commonly deployed are reported in the survey. A listing of the more popular security implementations are—Nmap, Aircrack-ng, WIFIphisher, Burp Suite, Social Engineer Toolkit, and Metasploit. The certification examinations that attract the highest mention are: Security+, Certified Information Systems Security Manager (CISM), Certified Ethical Hacker (CEH), and Risk and Information System Control (RISC).

A regression model consisting of three diagnostic variables and one independent variable (institution-related) was in turn, hypothesized. Model I F-tests of significance were used to assess changes in R^2 resulting from addition of each new set of predictors.

The negligible impact of institutional characteristics on course design and development is noteworthy. Factors such as school-type, accreditation status, and the deployment of cutting-edge IT infrastructure were tested against possible relationships to course emphasis, course activities and mode of instruction delivery. The results yielded no significant relationships, thus confirming the speculation that institution-related factors are not predictive of course design and structure when p is set at 0.05 (**Table 1**). The lack of relationship suggests that

there does seem to be the existence of a bench-mark Principles of Information Security course, at this point in time.

As for what instructional resources are used, the textbook titled Principles of Information Security by Michael Whitman and Herbert Mattod [10] appears to be most popular by simple frequency counts. Also, Cybersecurity by Dan Shoemaker and Arthur Conklin [7] and Fundamentals of Information Systems Security by David Kim and Michael Solomon [17] are at a distant second. Other popular textbooks shared a much smaller user base and their reported use is almost evenly distributed. One particular interesting question concerned the primary learning objective of the course. This question allowed participants to provide and elucidate open-ended responses.

A simple analysis of the feedback shown in **Table 2** depicts six (6) relevant areas. An overwhelming response (54 of 94 responses) reported emphasizing an understanding the application of Security to various Business functional Systems. For these instructors, the objective of the course was to provide an understanding of security implements and their deployments from strictly technical and professional standpoint. The second most popular response in this category (32 out of 94) is concerned with the need for students to understand the Security Systems Development Life Cycle (SecSDLC) aspect of Information Security Systems Development. As far as this cohort is concerned, the emphasis should be more on systems development, cyber literacy and hygiene, and merely gaining the language of the discipline, at the most basic proficiency level. Other areas that received below average mention include: the principles of the application of Cybersecurity; Networking Protocols and Threats; Access Control Methods and Models; and Computer Forensics and Investigations.

A question addressed what additional resources are required to better attain the teaching objectives. Of the 54 responses, approximately 70% strongly indicated

Table 1. Institutional variables vs. course design variables.

Institution-related Variables	Course Emphasis	Course Activities	Mode of Instruction Delivery
School Type	0.0092	0.1350	0.0723
Accreditation Status	0.1137	0.2211	0.1326
IT Infrastructure	0.1920	0.1423	0.0018

P = 0.05.

Table 2. Learning objectives of principles of information security course.

Topical Area	Frequency
Understanding the application of Security to various functional Business Systems	**54**
Understanding the Security Systems Development Life Cycle (SecSDLC) aspect of Information Security Systems Development	**32**
Learning the principles of the application of Cybersecurity	**17**
Networking Protocols and Threats	**13**

more intensive, practical, hands-on and simulation of real-life problem-solving strategy.

Greater than 30% of the sample expressed the need for installation of sophisticated, industrial-type equipment in the laboratories to facilitate effective delivery of course instructions. As partly addressed above on the recommendations for improving the course, four broad categories listed below were suggested:

1) the need to acquire better textbooks with case studies;

2) exposure to intense mimicry of real-life cyber threat and breach situations;

3) a practical, hands-on simulation of such scenarios; and

4) risk mitigation strategies and controls.

3.3. Qualitative Analysis

As indicated earlier, a multi-method data gathering approach was employed. The attractiveness of this strategy lies in the richness it adds to the data analysis process. Hence, data items were collected and coded using open and common themes in participants' responses.

Also, the need to use a multi-method data gathering approach prompted another purposive sampling which was geared towards providing a subjective yet complimentary source of data. This was dictated by the need to elicit additional information from course instructors to augment researchers' confidence in the questionnaire responses. 14 institutions (0.10%) of the survey sample), were targeted to be interviewed and have their course syllabi reviewed. Only 8 instructors cooperated fully. To get a more accurate idea of the nature and structure of the Principles course, course instructors were given latitude to express, in their own words, the descriptive elements of the course. Much congruence was reported.

For example, certain comments made in part are apt, that is:

1) "… Our focus in this course is primarily to expose our students to the conceptual foundations and operational tools of cybersecurity, and address risk and the improvement of cybersecurity posture of organizations."

2) "… It is incontrovertible that the major course here, is the Principles course. It prepares the students to be independent learners for all areas of information security and management."

Such anecdotes support the popular belief that standardizing a core Cybersecurity course would go a long way to filling the incongruence in the structure and format of the course and its delivery. The themes that revealed syllabi review, in order of precedence clearly, are cybersecurity, technology, risk management, human factors, policy, law, and ethics. As to be expected, different programs placed varying degrees of emphasis on the externalities which are deemed adjunct to the core cybersecurity core subject matter.

4. Conclusions

This study indicates that the structure and content of the Principles of Information Security courses are diverse and divergent. Although the study deals with

only a small sector of Cybersecurity pedagogy, the contributions of the research can be rich and varied. Furthermore, the findings make clear that the Principles of Information Security course refuses to be confined to a narrowly focused theme of technology or the pure non-technical domain of data and information protection. Instead, the course content covers a multilateral array of topics ranging from technology, human aspects of policy, education, training and awareness, in short, —the socio-technical dimensions of information and cybersecurity.

For one thing, some of its findings may be of interest to, and have implications for cybersecurity curriculum planning and management. The core objective of the study, which is to examine the nature and content of the Principles of Information Security course is established, in that, the results reveal an outcome serving as a definitive descriptive model for the typical Principles of Information Security course. Furthermore, apart from providing relevant and useful information regarding course content and format, it could further act as a meaningful basis for designing future Principles of Information Security course. Overall, what the study has demonstrated is the fullness of the Principles of Information Security course as glue that builds bridges between security, technology and the social intangible features of an organization. Overall, its contributions would be invaluable to the future improvement of Principles of information security course, design and development.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Adekoya, A.A. (2017) Carnegie African Diaspora Fellowship Program (CADFP): Final Report and Recommended Curriculum for the Master of Information Technology (MIT) Degree Program in Cybersecurity. Computer Sciences Department, University of Lagos, Lagos, Project ID: 00241602.

[2] Schneider, F.B. (2013) Cybersecurity Education in Universities. *IEEE Security & Privacy*, **11**, 3-4. https://doi.org/10.1109/MSP.2013.84

[3] Santos, H., Pereira, T. and Mendes, I. (2017) Challenges and Reflections in Designing Cyber Security Curriculum. 2017 *IEEE World Engineering Education Conference*, Santos, 47-51. https://doi.org/10.1109/EDUNINE.2017.7918179

[4] Fischer, E.A. (2009) Creating a National Framework for Cybersecurity: An Analysis of Issues and Options. Nova Science Publishers, New York.

[5] Alli, A. and Faraq, W. (2009) Introducing a Concentration in Information Assurance into a Computer Science Program. *Issues in Information Systems*, **10**, 185-193.

[6] Ayoub, R. (2011) The 2011 (ISC) 2 Global Information Security Workforce Study. ISC2, 2-27.

[7] Shoemaker, D. and Conklin, W.A. (2011) Cybersecurity: The Essential Body of Knowledge. Cengage Learning, Boston.

[8] ACM Computing Curricula Task Force (2013) Computer Science Curricula 2013:

Curriculum Guidelines for Undergraduate Degree Programs in Computer Science. ACM, Inc., New York. https://doi.org/10.1145/2534860

[9] Bogolea, B. and Wijekumar, K. (2004) Information Security Curriculum Creation: A Case Study. *Proceedings of the* 1*st Annual Conference on Information Security Curriculum Development*, Kennesaw, 59. https://doi.org/10.1145/1059524.1059537

[10] Whitman, M.E. and Mattord, H.J. (2004) Designing and Teaching Information Security Curriculum. *Proceedings of the* 1*st Annual Conference on Information Security Curriculum Development*, Kennesaw, 1. https://doi.org/10.1145/1059524.1059526

[11] Theoharidou, M. and Gritazalis, D. (2007) Common Body of Knowledge for Information Security. *IEEE Security and Privacy Magazine*, **5**, 64-67. https://doi.org/10.1109/MSP.2007.32

[12] Chin, S.K., Irvine, C.E. and Frincke, D. (1997) An Information Security Education Initiative for Engineering and Computer Science. Naval Postgraduate School Technical Report, NPSCS-97-003. Naval Postgraduate School, Monterey, CA. 12/1997, 59-65.

[13] Anderson, J.E. and Schwager, P.H. (2002) Security in the Information Systems Curriculum: Identification & Status of Relevant Issues. *Journal of Computer Information Systems*, **42**, 16-24.

[14] Crowley, E. (2003) Information System Security Curricula Development. *Proceeding of the* 4*th Conference on Information Technology Education*, Lafayette, 249. https://doi.org/10.1145/947121.947178

[15] Smith, T., Koohang, A. and Behling, R. (2010) Formulating an Effective Cybersecurity Curriculum. *Issues in Information Systems*, **11**, 410-416.

[16] Luallen, M.E. and Labruyere, J.-P. (2013) Developing a Critical Infrastructure and Control Systems Cybersecurity Curriculum. 2013 46*th Hawaii International Conference on System Sciences*, Wailea, 1782-1791. https://doi.org/10.1109/HICSS.2013.176

[17] Kim, D. and Solomon, M. (2018) Fundamentals of Information Systems Security. Third Edition, Jones & Bartlett Learning, Burlington.

[18] Anon (n.d.) How America Is Closing the Cybersecurity Skills Gap. Knowledge@Wharton. https://knowledge.wharton.upenn.edu/article/america-plans-close-skills-gap-cybersecurity

[19] Newhouse, W., Keith, S., Scribner, B. and Witte, G. (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. National Institute of Standards and Technology, Gaithersburg, NIST SP 800-181. https://doi.org/10.6028/NIST.SP.800-181

[20] Burley, D.L., *et al.* (2017) The Joint Task Force on Cybersecurity Education. *Twenty Second Americas Conference on Information Systems,* San Diego, CA, 31 December 2017, 23-24.