SAIS 2012 Proceedings

Southern (SAIS)

2012

The Importance of Acquiring the Security Domains' Knowledge and Skills in Students' Educational Experience

Tina Ashford
Macon State College, Macon, GA, tina.ashford@maconstate.edu

Kevin Floyd
Macon State College, Macon, GA, kevin.floyd@mga.edu

Alex Koohang
Macon State College, Macon, GA, alex.koohang@maconstate.edu

THE IMPORTANCE OF ACQUIRING THE SECURITY DOMAINS' KNOWLEDGE AND SKILLS IN STUDENTS' EDUCATIONAL EXPERIENCE

Tina Ashford
Macon State College, Macon, GA
tina.ashford@maconstate.edu

Kevin Floyd
Macon State College, Macon, GA
kevin.floyd@maconstate.edu

Alex Koohang
Macon State College, Macon, GA
alex.koohang@maconstate.edu

ABSTRACT

The primary purpose of this study was to gather information about students' opinion regarding the importance of acquiring security domains' knowledge and skills in their educational experience. These students were males and females with various age groups studying in a four-year information technology program with a concentration in information assurance and security in a medium-sized institution in the southeast USA. Collected data were analyzed and results are presented. Conclusion and recommendations complete the paper.

Keywords

Security domains, information security, cybersecurity, educational experience

INTRODUCTION

Fischer (2005) defined cybersecurity as 1) "measures to protect information technology; the information it contains, processes, and transmits and associated physical and virtual elements (which together comprise cyberspace)"; 2) "the degree of protection resulting from application of those measures; and 3) "the associated field of professional endeavor."

The Congressional bill of the cybersecurity Act of 2009 highlights “continued free flow of commerce within the United States and with its global trading partners through secure cyber communications, to provide for the continued development and exploitation of the Internet and intranet communications for such purposes, to provide for the development of a cadre of information technology specialists to improve and maintain effective cybersecurity defenses against disruption, and for other purposes.” (http://www.opencongress.org/bill/111-s773/show)

Werlinger, Hawkey and Beznosov (2009) stated that the lack of security training, the lack of a security culture, ineffective security risk estimation, the complexity of security systems, and a lack of security tools are the most critical challenges for organizations; and that there is an immediate need for IT security specialists who understand the security threats.

A recent survey by Frost and Sullivan sponsored by (ISC)2 revealed that information security professionals lack appropriate skills for protecting organizations' against various cybesecurity treats (Ayoub, 2011).

In this survey, some key findings included the following:

1. Application vulnerabilities represent the number one threat to organizations.
2. Mobile devices were the second highest security concern for the organization
3. Professionals aren’t ready for social media threats
4. Cloud computing illustrates a serious gap between technology implementation and the skills necessary to provide security
5. A clear skills gap exists that jeopardizes professionals’ ability to protect organizations in the near future (Ayoub, 2011).

Furthermore, the survey stated: "The information security profession could be on a dangerous course, where information security professionals are engulfed in their current job duties and responsibilities, leaving them ill-prepared for the major changes ahead, and potentially endangering the organizations they secure." (Ayoub, 2011)

Smith, Koohang and Behling (2010) stated that professional organization that offer information security certification programs can provide assurance that certified individuals have minimum competencies, skills and experience in cybersecurity.

Several organizations offer certification programs that are universally accepted. Examples of these organizations are 1) International Information Systems Certification Consortium (ISC) 2; 2) Global Information Assurance Certification (GIAC); and 3) Microsoft Corporation.

Smith, Koohang and Behling (2010) further delineated the critical role of higher education institutions that offer cybersecurity program in preparing students to acquire necessary knowledge and skills to be competitive when taking certification examinations. The authors advanced a model for designing cybersecurity curriculum that included formulating program mission, constructing program career goals, and determining program competencies. The program competencies were derived from (ISC)2 "10 security domains". These security domains offer a universal body of knowledge for information security professionals and provide a foundation for security practices and principals in all industries. They are as follows:

1. Security management practices
2. Access control systems and methodology
3. Telecommunications and networking security
4. Cryptography
5. Security architecture and models
6. Operations security
7. Application and systems development security
8. Physical security
9. Business continuity and disaster recovery planning
10. Laws, investigation, and ethics (ISC, http://www.isc2.org)

Therefore, the cybersecurity program competencies proposed by Smith, Koohang and Behling (2010) included 10 competencies that should be required of students to have by the time of graduation. These competencies are as follows:

1. An ability to demonstrate and apply security management practices
2. An ability to identify access control systems and methodology
3. An ability to describe telecommunications and networking security
4. An ability to use and apply current techniques, skills, and tools necessary for cryptography
5. An ability to identify and apply security architecture and models
6. An ability to identify current techniques and tools necessary for operations security
7. An ability to identify and analyze application and systems development security
8. An ability to identify and use physical security
9. An ability to identify and apply business continuity and disaster recovery planning
10. An ability to describe and apply security laws, investigation, and ethics (Smith et al., 2010).

PURPOSE OF THE STUDY

There are 10 security domains created by the International Information Systems Security Certification Consortium ((ISC)2, http://www.isc2.org)) to: 1) offer a universal body of knowledge for information security professionals; and 2) provide a foundation for security practices and principals. The purpose of this survey was to gather students' opinion about the importance of acquiring each of these security domains in their educational experience. Two research questions were formed:

- **RQ1:** Is there a difference between students' age and their opinion about the importance of the security domains in their educational experience**?**
- **RQ2:** Is there a difference between student' gender and their opinion about the importance of the security domains in their educational experience?

Gender was selected as a variable because the underrepresentation of women in IT has been reported in various studies. The IT remains a heavily male-dominated discipline (Trauth, Quesenberry and Yeo, 2008). Furthermore, women exhibit significantly lower computer self-efficacy and higher anxiety toward computers than men (Roach, McGaughey and Downey, 2011). This may be true when determining whether there are differences between male and female in respect with their opinion about the importance of the security domains in their educational experience.

Age was selected as a variable because the observations of the authors of this study in their institution had revealed that students of all ages -- from incoming freshmen directly from high school to older returning students -- are enrolling in the information assurance and security program. Therefore, it would be worthwhile to find out if there are differences among students' age and their opinion about the importance of the security domains in their educational experience; and how these differences may play an important role in receptivity to information assurance and security program among students.

METHODOLOGY

Instrument Survey

The Likert-type survey instrument consisted of the 10 security domains advanced by (ISC)2. The items were as follows:

1. Information Security governance and risk management (Identifying vulnerabilities in an organization's information system)
2. Access control (How access rights are granted to entities.)
3. Telecommunications and networking security (Providing confidentiality, integrity, and accessibility to the network infrastructure.)
4. Cryptography (The enciphering and deciphering of coded data.)
5. Security architecture and Design (Planning and developing of security policies and procedures.)
6. Operations security (Safeguarding of the organization's ability to support operational activities)
7. Application development security (Ensuring the integrity of applications and programming personnel.)
8. Physical (Environmental) security (Protection of the physical resources of an organization.)
9. Business continuity and disaster recovery planning (Ensuring the continuation and recovery of business activities in the event of a catastrophe.)
10. Legal, regulations, investigations, ethics and compliance (Covers all legal and ethical issues associated with information security.)

The instrument used the following scoring strategy: 4 = Critical, 3 = Important, 2 = Somewhat important, and 1 = Not important

Sample and Procedure

The survey was administered to 87 students who were enrolled in a four-year undergraduate information technology program with a concentration in information assurance and security in a mid-sized higher education institution located in the southeast United States. The survey was approved by the IRB with exempt status. Subjects were males and females in various age groups - 1) 18– 23 Years, 2) 24 – 29 Years, 3) 30 – 35 Years, 4) 36 – 41 Years, and 5) Over 41 Years. The subjects were taking the following courses: foundation of information assurance & security; information security law & ethics; computer forensics; incident disaster recovery & business continuity; and application development. These courses were all required for the information assurance & security major concentration in the program.

The participants were 18 years and older. They were assured protection of their anonymity. Of the 87 surveys, 3 were eliminated because of incomplete data. This yielded a final sample of 84 participants.

Data Analysis

Data were collected and analyzed by a popular statistical software known as SPSS. Analyses included descriptives and two separate one-way analysis of variance (ANOVA). ANOVA was used to test differences between means of two or more groups. It uses the F statistic to test the statistical significance of the differences among the means. The predetermined level of significance, .05, was used.

RESULTS

Descriptives

All security domains received high mean scores - above 3.3 (the mid-point score was 2.5). This indicated that students had high to very high opinion about the importance of each of these security domains in their educational experience. The list below shows the security domains' results from high to low. (Also see Figure 1 for the graphic representation)

1. Telecommunications and networking security (Providing confidentiality, integrity, and accessibility to the network infrastructure.)
2. Information Security governance and risk management (Identifying vulnerabilities in an organization's information system.)

3. Business continuity and disaster recovery planning (Ensuring the continuation and recovery of business activities in the event of a catastrophe.)
4. Access control (How access rights are granted to entities.)
5. Security architecture and Design (Planning and developing of security policies and procedures.)
6. Operations security (Safeguarding of the organization’s ability to support operational activities without
7. Physical (Environmental) security (Protection of the physical resources of an organization.)
8. Cryptography (The enciphering and deciphering of coded data.)
9. Application development security (Ensuring the integrity of applications and programming personnel.)
10. Legal, regulations, investigations, ethics and compliance (Covers all legal and ethical issues associated with information security.)

RQ1: Is there a difference between students’ age and their opinion about the importance of the security domains in their educational experience**?** The results of ANOVA indicated that there was a significant difference between the levels of age and their opinion regarding the importance of the security domains in their educational experience (See Table 1). An analysis of the means among the level of age indicates that older students had more positive opinions toward the security domains in their educational experience (See Table 2).

	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Between Groups (Combined)	1.000	4	.250	2.534	.047
Within Groups	7.793	79	.099		
Total	8.792	83			

Table 1. ANOVA for Security Domains and Age

Age	Mean	N	SD
18– 23	3.4143	35	.28506
24 – 29	3.6250	20	.31933
30 – 35	3.6500	12	.30302
36 – 41	3.4444	9	.42459
Over 41	3.6500	8	.30237
Total	3.5238	84	.32547

Table 2. Descriptives for Security Domains and Age

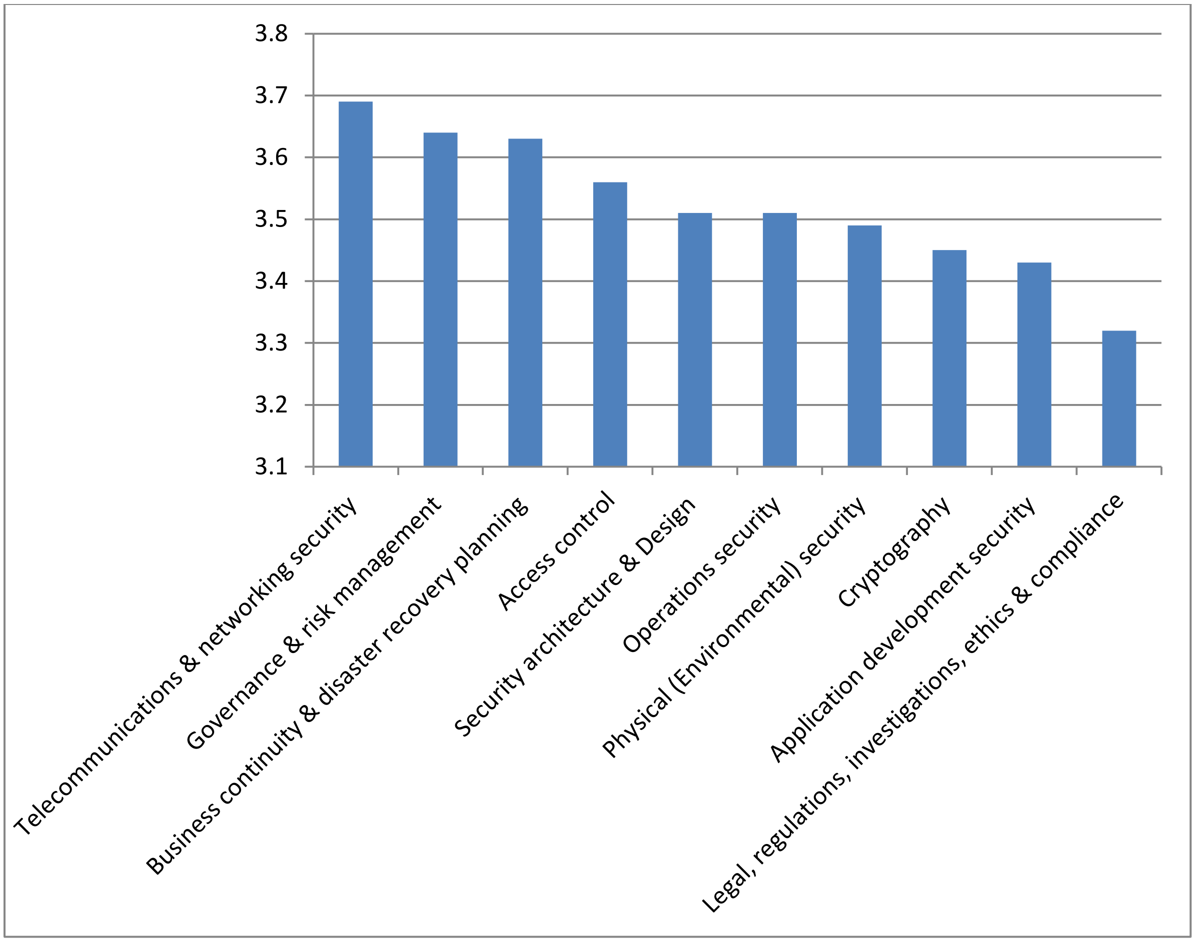

Figure 1. Graphic Representation of Each Security Domain Means from High to Low

RQ2: Is there a difference between learners' gender and their opinion about the importance of the security domains in their educational experience? The results of ANOVA for gender indicated no significant difference between males and females and their opinion regarding the importance of the security domains in their educational experience (See Table 3). Table 4 shows the means and standard deviation.

	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Between Groups (Combined)	.026	1	.026	.239	.626
Within Groups	8.767	82	.107		
Total	8.792	83			

Table 3. ANOVA for Security Domains and Gender

Gender	Mean	N	SD
1	3. 5141	64	.32556
2	3.5550	20	.33162
Total	3.5238	84	.32547

Table 4. Descriptives for Security Domains and Gender

CONCLUSION

The results of this study show that students find the topics of Cybersecurity and Information Assurance to be very important. With this in mind, institutions of higher learning should take these topics into careful consideration when designing their Cybersecurity and Information Assurance curriculum. Building upon the previous research by Smith et al. (2010) and the findings of this study, the authors of the present study suggest that, at a minimum, six courses should be required in a Cybersecurity and Information Assurance program to cover the knowledge and skills of the 10 security domains. These courses are 1) business continuity and disaster recovery planning; 2) client/server systems security; 3) information security management; 4) legal and ethical issues of information security; 5) network security; and software security. For an in-depth view of a Cybersecurity program, including the course topics and learning outcomes refer to (Smith et al., 2010). In addition, an overview course in cybersecurity foundation is recommended to cover the prerequisites for the six courses in the program.

The results of ANOVA for gender indicated no significant difference between male and female. Male and female students had equally positive opinion toward acquiring the security domains' knowledge and skills in their educational experience.

The significant difference among the age groups of 1) 18 - 23, 2) 24 - 29, and 3) 30 - 35 clearly indicated that the older the students, the higher the mean score. This means that older students had more positive opinion toward acquiring the security domains' knowledge and skills in their educational experience. Likewise, there was a significant difference among the levels of the means of the age group 1) 36 - 41 and 2) over 41 showing that students who were above the age of 41 had more positive opinion toward acquiring the security domains' knowledge and skills in their educational experience.

As can be seen, there was a drop in the mean score between the 30 - 35 and 36 - 41 age groups following a spike with those over the age of 41. A possible explanation of that age group’s recognition of the importance of security domains is the increased attention of security-related events since the early 2000s. This age group would have been in their early 20s during many of the national security events of that time and therefore made more aware of Cybersecurity and Information Assurance issues. This notion perhaps requires further study.

The results of this study, in general, indicate that students are not only aware of Cybersecurity and Information Assurance, but recognize the importance of the same. This study recommends that Cybersecurity and Information Assurance curriculum should be designed to include all the 10 security domains knowledge and skills that prepare students for many challenges in Cybersecurity and Information Assurance.

REFERENCES

1. Ayoub, R. (2011) The 2011 (ISC)2 Global Information Security Workforce Study, *Frost & Sullivan.* Retrieved November 5, 2011 from https://www.isc2.org/uploadedFiles/Landing_Pages/NO_form/2011GISWS.pdf
2. Fischer, Eric A. (2005) Creating a National Framework for Cybersecurity: An Analysis of Issues and Options, February 22, CRS Report for Congress, Order Code RL32777. URL: http://www.usembassy.it/pdf/other/RL32777.pdf [last accessed on 10 June 2005].
3. Smith, T., Koohang, A. and Behling, R. (2010) Formulating an effective cybersecurity curriculum, *Issues in Information Systems*, 11(1), 410-416.
4. Roach, D., McGaughey, R. and Downey, J. (2011) Gender within the IT major – a retrospective study of factors that lead students to select an IT major, *International Journal of Business Information Systems*, 7(2).
5. Trauth, E. Quesenberry, J. and Yeo, B. (2008) Environmental influences on gender in the IT workforce. *Newsletter: ACM SIGMIS Database Archive*, 39(1).
6. Werlinger, R. W., Hawkey, K. and Beznosov, K. (2009) An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, 17(1), 4-19.