European Journal of Business and Social Sciences, Vol. 1, No. 6, pp 46-55, **October 2012.**
URL: *http://www.ejbss.com/recent.aspx*
ISSN: 2235 -767X

SECURITY EDUCATION IN COLLEGES: IS IT SUFFICIENT?

Mark Ciampa

Western Kentucky University
1906 College Heights Boulevard,
Bowling Green, KY 42101

Ray Blankenship

Western Kentucky University
1906 College Heights Boulevard,
Bowling Green, KY 42101

Email: Ray.Blankenship@wku.edu
Tel: 1-270-745-5952 (USA)

ABSTRACT

As attacks on computer security continue to increase it is important that security awareness, education, and training be used as an important defense, and increasingly colleges are being looked upon to provide this instruction. Yet an examination of higher education regional accrediting bodies and accrediting agencies for colleges of business indicate that there are no specific requirements that current security topics be taught in the curriculum. A random sample of the Association to Advance Collegiate Schools of Business (AACSB) accredited schools shows that fewer than half teach any computer security topics to college of business students. This is despite the fact that a survey of students indicates that they are indeed concerned about security; however, these concerns are not being met. The results of this study can be used by faculty and administrators to work towards creating standards and improving computer literacy courses where computer security is not being taught. (Keywords: computer security, pedagogy, business education, & accreditation)

Introduction

Computer security continues to be a primary concern of all computer users today. The breadth and depth of attacks is such that it now impacts all economic sectors, units of government, and individuals. For example, the number of malware attacks against online banking is increasing annually by 60,000, and 85 percent of banks reported that they have sustained losses based on these attacks (Lohrmann, 2010). Over $41 billion dollars have been lost by victims to the Nigerian General scam, which is the number one type of Internet fraud and is growing at a rate of 5 percent (419 Advance fee fraud statistics 2009, 2010). Over 20 million new specimens of malware, including new malware as well as variants of existing families, were created a single eight-month period, and the average number of new threats created and distributed each day has increased from 55,000 to 63,000 (Santana, 2011). And due to the increased power of desktop computers to crack passwords, researchers now claim that any password of seven or fewer characters is "hopelessly inadequate" (Case Study - Teraflop troubles: The power of graphics processing units may threaten the world's password security system).

It is recognized that technology alone cannot prevent attacks; instead, security awareness, education, and training is a critical defense component (Ciampa, 2011). A growing number of entities are calling for this security training to be part of an overall college experience for all users and not limited to those students seeking a degree in information technology security. For example, the U.S. National Institute of Standards and Technology (NIST) draft National Initiative for Cybersecurity Education (NICE) plan, which came from the White House's Comprehensive National Cybersecurity Initiative of 2008, has as its goal is to improve cybersecurity by focusing on education, awareness and training. A strategy for Objective 1.1 is to "deliver resources that enable educators to competently communicate cybersecurity awareness to students during all classroom interactions with cyberspace" (National Initiative for Cybersecurity Education, 2011).

The current questions become, what are colleges and universities doing in providing computer security instruction as a requirement for higher level education? Do higher education regional accrediting bodies and/or accrediting agencies for colleges of business require security education, and if so, what is it? How many colleges are teaching about computer security? What security topics are most important? And do students even care about learning security?

The purpose of this paper is to take a random sample of the Association to Advance Collegiate Schools of Business (AACSB) accredited schools and determine what--if any--computer security topics are being taught to college of business students. In addition, in order to establish a baseline of what students consider important, a survey of students at university and community college was conducted regarding their perceptions of the importance of specific security topics.

Literature Review

A comprehensive model of information security was originally developed for the National Security Telecommunications Information Systems Security Committee (NSTISSC) and is known as the Comprehensive Model for Information Systems Security or the C.I.A. triad (Mensch & Wilkie, 2011). The three critical characteristics of information in this model are: confidentiality, integrity, and availability (NSTISSC, 1994). It is these characteristics that users need to be informed about trained to understand. The need for security training is emphasized by many researchers because it is frequently maintained that the user is weakest link in computer security, by Long (1999), Mangus (2002), Tobin and Ware (2005), Werner (2005), Witson (2003), Yang (2001) and others. Observations ranged from a mild statement of "certain user practices contribute to information systems vulnerabilities" by Mangus (2002) to a sharp rebuke of "the average home user is clueless about security and should be required to obtain a license to log on to the internet" by Werner (2005). Werner indicated that support for pointing a finger at users is found in a National Cyber Security Alliance (NCSA) and American Online (AOL) survey, in which 77 percent of respondents indicated that they felt safe from online threats. However, when their computers were actually inspected, over 20 percent of computers were infected with at least one virus, 49 percent of broadband users

lacked firewall protection, 67 percent of computers lacked current anti-virus software, and 80 percent of computers were infected with spyware or adware (Werner, 2005).

Valentine (2005) noted that the National Strategy to Secure Cyberspace (NSSC) document, created by the U.S. President's National Infrastructure Advisory Council, calls for a comprehensive national awareness program to empower all Americans, including the general population, "to secure their own parts of cyberspace." Specifically, the Department of Homeland Security, through the NSSC, calls upon home users to help the nation secure cyberspace "by securing their own connections to it."

Educating general users on security also has additional benefits. First, it can provide future users with the critical thinking and basic skills to collaborate with vendors and IT professionals who provide security tools (Werner, 2005). A second benefit is that it may serve to deter attackers. Long (1999) stated that countermeasure strategies to reduce systems risk fall into four distinct and sequential activities: deterrence, prevention, detection, and recovery. General deterrence theory has been used in the study of criminals and other anti-social personalities and maintains that individuals with an instrumental intent to commit anti-social acts can be dissuaded by the administration of strong disincentives and sanctions relevant to these acts. General deterrence theory has also been applied successfully to IT by Straub (1990) and Straub, Carlson and Jones (1993). Educating users can be a form of deterrence by providing information about the risks of security and penal actions that can be taken against attackers.

The benefit of training and instruction to deter attackers can also be seen in other studies. Skinner and Fream (1997) used social learning theory as a framework for exploring computer crime and security among college students. Social learning theory is organized around four concepts, one of which is differential association. Differential association refers to the process by which individuals within different social contexts become exposed to learn normative definitions favorable and unfavorable to legal and illegal (Mangus, 2002). Analysis revealed strong support for social learning theory as a conceptual framework for understanding computer crime (Skinner & Fream, 1997). One of the major predictors of computer crime was associating with other students who engage in the activity, meaning that learning computer crime is peer driven. Training and instruction regarding computer security may prove to be a deterrent not only to primary individuals but also secondarily by reducing the peer support for attacking systems.

Although Long (1999) advocated that security instruction should begin as early as kindergarten, most researchers state that institutions of higher education (IHEs) should be responsible for providing security awareness instruction, including Crowley (2003), Mangus (2002), Null (2004), Tobin and Ware (2005), Valentine (2005), Werner (2005), and Yang (2001). This instruction and training is important not only to meet the current demands of securing systems but also to prepare students for employment in their respective fields. Werner said that as employees, new college graduates will have access to critical data to perform their jobs, yet they could be the weakest link in a secure computer system primarily because of inadequate education, negligence, and inexperience (2005). Long (1999) maintained that the need for organizations to develop appropriate policies requires all decision makers to have a certain level of awareness of standards for security.

Support for making IHEs the primary source for security awareness training comes from several different sources. The Action and Recommendation 3-4 of the NSSC calls upon colleges and universities to model user awareness programs and materials (Valentine, 2005). Frincke and Bishop (2004) summarized several of the major groups and efforts currently involved in computer security education with IHEs. These include the Colloquium for Information Systems Security Education (CISSE), the International Federation of Information Processing Working Group 11.8 on Information Security Education (IFIP WISE), and the Workshop on Education in Computer Security (WECS). The National Security Agency (NSA) also had developed an effort aimed at creating a larger core of computer security trained professionals known as the National Centers of Academic Excellence in Information Assurance Education, which even provides large numbers of college scholarships under its "Cyber Corps" program.

The location of security awareness instruction and training in a college curriculum should not be isolated in upper-level courses for IT majors, according to Tobin and Ware (2005), Werner (2005), and others. This instruction should be taught to all graduates as a "security awareness" course (Valentine, 2005) along with integrating it across through the curriculum (Yang, 2001).

Different approaches exist for training and educating users regarding security. These approaches can be classified as contextual training and embedded training (Sheng, et al., 2007).

Contextual training involves incidences of instruction separate from the course of normal activities. One common approach is to post articles regarding fishing on Websites and encourage users to read them. E-commerce sites (Tutorial spoof (fake) e-mail), software vendors (Recognizing phishing scams and fraudulent/hoax e-mails, 2006), nonprofit organizations (Consumer advice: How to avoid phishing scams), universities (Anti-phishing Phil) and government entities (How not to get hooked by a 'phishing' scam, 2006) all post anti-phishing material.

Embedded training involves instruction during the course of normal activities. Kumaraguru et al. (2007) recommended that instead of sending periodic security notices to users, organizations should use an embedded training approach that teaches users how to protect themselves from phishing during their regular use of e-mail. In this approach, users were periodically sent fake phishing e-mails from the researchers; if a user clicked on an embedded link an intervention that provided immediate feedback and steps that the user should have taken appeared.

Methodology

The purpose of this study is to take a random sample of accredited schools to determine the computer security topics that are being taught. In addition, in order to establish a baseline of what students consider important, a survey of students at a university and community college was conducted regarding their perceptions of the importance of specific security topics.

Several higher education accrediting bodies all require that students be exposed to the use of current technology in society. These include the New England Association of Schools and Colleges Commission on Institutions of Higher Education (NEASC-CIHE) (Standards for accreditation - 2011, 2011), the Southern Association of Colleges and Schools (SACS), and the North Central Association of Colleges and Schools (NCA) (North Central Association Resources, 2011). However, there are no specific requirements for computer security as it pertains to the use of technology. Accrediting agencies exist for colleges of business such as the Accreditation Council for Business Schools and Programs (ACBSP) (ACBSP standards and criteria for demonstrating excellence in baccalaureate/graduate degree schools and programs - 2011, 2011), International Assembly for Collegiate Business Education (IACBE) (Self-study manual - 2011, 2011), and the AACSB (AACSB eligibility procedures and acreditation standards for business accreditation association to advance collegiate schools of business, 2011). Again, these agencies also require that the most current technology be taught to business students but there are no specific requirements that current security topics be taught in the curriculum.

A random selection of AACSB accredited schools were selected for this study because of the explicit technology requirements stated in the standards by this accrediting agency.

To establish a baseline of what students consider to be an important security topic a group of information technology experts were asked to list what computer security topics should students know. The agreed upon topics are using anti-virus software, using a firewall, security wireless networks, using spam filters, and protection from phishing. Students where then asked to rank the importance of these topics on a Likert scale from 1 (Very Important) to 6 (Unfamiliar with the Topic).

Results

A survey was conducted of students at a mid-western university and community college. In order to minimize any influence on student responses, the survey was conducted on the first day of an *Introduction to Computers* course. Students had received no prior instruction about security and had no previous computer courses at their school. They were asked if specific security items were important to them.

The number of students participating in this survey was 348. The age ranged from 17-58 and there were 183 males and 165 females. Table 1 lists the number of student responses for each topic. Table 2 lists the percentage response for the topics.

To determine what security topics are being taught in AACSB accredited business schools a random sample of 32 business schools were selected from the list of AACSB accredited business schools that have their required technology course syllabi listed on the Web. The syllabi were then analyzed to see what computer security topics were covered in these classes. Table 3 lists the results of this analysis.

Discussion

Students in the survey clearly indicated that security was an important topic. Over 90 percent of the students said that using anti-virus software was an important or very important security topic. Securing wireless networks was second with 89.5 percent of the student stating that this was a very important or important security topic. The remaining topics were considered important or very important by over four out of five of the students. These findings are consistent with the recommendations of the technology experts who listed these topics as important for students to know. An interesting finding in this area is that nearly 8 percent of the students were unfamiliar with the topic of phishing and additionally almost 7 percent of the students were neutral about whether this topic is important or not. Phishing appears to be a security topic with which students are the most unfamiliar.

When syllabi were analyzed to see what type of security topics were being covered in a required computer class for an AACSB accredited schools no specific information could be found. Fewer than half of the syllabi examined mentioned any security being taught at all in the classroom. This would seem to indicate that many schools may not be teaching students about computer security and how to prevent harmful attacks from outsiders. Since these results are for a business college where a computer technology course is required the authors can only assume that the results for other colleges would be much worse where there is no computer technology requirement for their curriculum.

Recommendations

Due to the steady increase of attacks security awareness, education and training are becoming increasingly important. Colleges and universities are being viewed as one of the primary sources for conducting this training for all students. However, our study indicates that there is a serious lack of education in computer security among colleges. The survey results from students strongly indicate that students are concerned about security and may be looking to colleges for that training—yet it is not to be found.

It is recommended that the higher education regional accrediting bodies and accrediting agencies for colleges of business work to establish minimum standards of computer security instruction. This would help provide users with the skills and knowledge they need to use technology in a responsible and safe fashion, both at home as well as on the job.

Another recommendation is that colleges examine their curriculums and begin to identify areas in which computer security education can take place. Suggestions include an *Introduction to Computers* course, a freshman orientation course, a one-hour technology safety course, or similar area.

Finally, it is recommended that additional study be conducted regarding what security topics students are the most deficient in. In our study nearly 8 percent of the students were unfamiliar with the topic of phishing and additionally almost 7 percent of the students were neutral about whether this topic is important or not. Phishing appears to be a security topic with which students are the most unfamiliar and thus this topic, along with other topics, need special attention in training.

Works Cited

How not to get hooked by a 'phishing' scam. (2006, October). Retrieved December 12, 2007, from Federal Trade Commission: http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm

Recognizing phishing scams and fraudulent/hoax e-mails. (2006, September 14). Retrieved December 12, 2007, from Microsoft: http://www.microsoft.com/protect/yourself/phishing/identify.mspx

419 Advance fee fraud statistics 2009. (2010, January). Retrieved February 2011, 2011, from Ultrascan-agi: www.ultrascan-agi.com/public_html/html/public_research_reports.html

AACSB eligibility procedures and acreditation standards for business accreditation association to advance collegiate schools of business. (2011, January). Retrieved August 15, 2011, from AACSB: http://www.aacsb.edu/accreditation/standards-2011-revisions-jan2011.pdf

ACBSP standards and criteria for demonstrating excellence in baccalaureate/graduate degree schools and programs - 2011. (2011). Retrieved August 15, 2011, from Accreditation council for business schools and programs: http://www.acbsp.org/download.php?sid=29

(2011). *National Initiative for Cybersecurity Education.* Washington: National Institute of Standards and Technology.

North Central Association Resources. (2011). Retrieved August 15, 2011, from North Central Association: http://www.ncacasi.org/resources/

Self-study manual - 2011. (2011). Retrieved August 15, 2011, from International Assembly for Collegiate Business Education: http://www.iacbe.org/doc/self-study-manual-10.doc

Standards for accreditation - 2011. (2011). Retrieved August 15, 2011, from New England association of schools and colleges commission on institutes of higher education: http://cihe.neasc.org/standards_policies/standards/standards_html_version

Anti-phishing Phil. (n.d.). Retrieved December 12, 2007, from CMU Usable Privacy and Security Laboratory: http://cups.cs.cmu.edu/antiphishing_phil/

Case Study - Teraflop troubles: The power of graphics processing units may threaten the world's password security system. (n.d.). Retrieved February 28, 2011, from Georgia Tech research institute: http://www.gtri.gatech.edu/casestudy/Teraflop-Troubles-Power-Graphics-Processing-Units-GPUs-Password-Security-System

Ciampa, M. (2011). *Security+ guide to network security fundamentals 4ed*. Boston: Course Technology.

Committee, N. S. (1994, June). *The Committee on National Security Systems.* Retrieved January 25, 2012, from http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf

Consumer advice: How to avoid phishing scams. (n.d.). Retrieved December 12, 2007, from Anti-Phishing Working Group: http://www.antiphishing.org/consumer_recs.html

Crowley, E. (2003). Information systems security curricular development. *Conference on Information Technology Education* (pp. 249-255). Lafayette, IN: ACM.

Frincke, D., & Bishop, M. (2004). Joining the security education community. *IEEE Security and Privacy, 2*(5), 61-63.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting people from phishing: the design and evaluation of an embedded training e-mail system. *CHI 2007 Procedeedings* (pp. 905-914). San Jose: ACM.

Lohrmann, D. (2010, July 30). *Should governments join banks in seeking customer's help online?* Retrieved February 28, 2011, from Government Technology Blogs: http://www.govtechblogs.com/lohrmann_on_infrastructure/2010/07/should-governments-join-banks.php

Long, C. L. (1999). A socio-technical perspective on information security knowledge and attitudes. *Ph.D. dissertation, The University of Texas at Austin, United States-- Texas*.

Mangus, T. (2002). A study of first-year community college students and proposed responsible computing guide. *Ph.D. dissertation, Union Institute and University, United States--Ohio*.

Mensch, S. &. (2011). Information Secutiy Activities of College Students: An Exploritory Study. *Academy of Information and Managment Science Journal, 14*(2), 91-116.

Null, L. (2004). Integrating security across a computer science curriculum. *Journal of Competing Science is in Colleges, 19*(5), 170-178.

Santana, J. (2011, January 25). *Panda security insight blog*. Retrieved February 28, 2011, from European commission suspends CO2 credit trading due to cyberattack: http://www.pandainsight.com/en/

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., et al. (2007). Anti-phishing Phil: The design and evaluation a game that teaches people not to fall for phish. *Symposium On Usable Privacy and Security*. Pittsburgh, PA: CMU.

Skinner, W., & Fream, A. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency, 34*, 495-518.

Straub, D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly*, 45-55.

Straub, D. W., Carlson, P., & Jones, E. (1993). Deterring cheating by student programmers: A field experiment in computer science. *Journal of Management, 5*, 33-48.

Tobin, D., & Ware, M. (2005). Using a windows attack intRusion emulator (AWARE) to teach computer security awareness. *10th Annual SIGSCE Conference on Innovation and Technology in Computer Signs Education* (pp. 213-217). Caparica, Portugal: SIGSCE.

Tutorial spoof (fake) e-mail. (n.d.). Retrieved December 12, 2007, from eBay: http://pages.ebay.com/education/spooftutorial/

Valentine, D. W. (2005). Practical computer security: A new service course based upon the national strategy to secure cyberspace. *Conference on Information Technology Education* (pp. 185-189). Newark, NJ: ACM.

Werner, L. (2005). Redefining computer literacy in the age of ubiquitous computing. *Conference on Information Technology Education* (pp. 95-99). Newark, NJ: ACM.

Whitson, G. (2003). Computer security: Theory, process and management. *Journal of computing sciences in colleges, 18*(6), 57-66.

Yang, T. A. (2001). Computer security an impact on computer science education. *Journal of Computing Sciences in Colleges, 18*(6), 233-246.

Table 1: Importance of Security Topics

Topic	Very Important	Important	Neutral	Somewhat Unimportant	Unimportant	Unfamiliar with Topic	Responses
Using anti-virus software	223	102	15	2	1	2	345
Using a firewall	154	142	33	3	3	10	345
Securing wireless networks	191	117	28	3	2	3	344
Using spam filters	156	138	34	4	4	8	344
Protecting yourself from phishing	176	114	23	1	2	27	343

Table 2: Importance of Security Topic by Percentage Response

Topic	Very Important	Important	Neutral	Somewhat Unimportant	Unimportant	Unfamiliar with Topic
Using anti-virus software	64.6%	29.6%	4.3%	0.6%	0.3%	0.6%
Using a firewall	44.6%	41.2%	9.6%	0.9%	0.9%	2.9%
Securing wireless networks	55.5%	34.0%	8.1%	0.9%	0.6%	0.9%
Using spam filters	45.3%	40.1%	9.9%	1.2%	1.2%	2.3%
Protecting yourself from phishing	51.3%	33.2%	6.7%	0.3%	0.6%	7.9%

Table 3: Syllabi Topics Covered in an Introduction to Computers Class Taught in an AACSB Accredited School

Topics	# of Schools that covered the topic	Percentage
Excel	22	68.8%
Access	22	68.8%
Hardware	17	53.1%
software	17	53.1%
Ethical Topics	17	53.1%
Networking	15	46.9%
Security	15	46.9%
PowerPoint	13	40.6%
Word	12	37.5%
internet	12	37.5%
Databases	11	34.4%
Strategic Role of IS	10	31.3%
HTML	9	28.1%
Ecommerce	9	28.1%
SDLC	8	25.0%
Database Queries	7	21.9%
OS	7	21.9%
Email	6	18.8%
Knowledge Management	5	15.6%
Programming	4	12.5%
Customer Relationship Management	4	12.5%
ERP	4	12.5%
Dream Weaver	3	9.4%
Supply Chain Management	3	9.4%
Content Management Systems	1	3.1%
Expression w\Web	1	3.1%
Desk Top Publishing	1	3.1%
AI DSS	1	3.1%
Computer Crime	1	3.1%
Collaborative tools	1	3.1%