Incorporating Global Information Security and Assurance in I.S. Education

Garry L. White, CCP, CISSP, Ph.D.
Department of Computer Information Systems and Quantitative Methods
McCoy College of Business
Texas State University
San Marcos, TX
gw06@txsstate.edu

Barbara Hewitt, Ph.D.
Computer Information Systems
College of Business
Texas A&M University-San Antonio
San Antonio, TX
bhewitt@tamusa.tamus.edu

S. E. Kruck, Ph.D., CPA, CCP
Computer Information Systems Department
College of Business
James Madison University
Harrisonburg, VA
kruckse@jmu.edu

ABSTRACT

Over the years, the news media has reported numerous information security incidents. Because of identity theft, terrorism, and other criminal activities, President Obama has made information security a national priority. Not only is information security and assurance an American priority, it is also a global issue. This paper discusses the importance of Global Information Security and Assurance in information systems (IS) education.

Current university graduates will become tomorrow's users and protectors of data and systems. It is important for universities to provide training in security and assurance of information systems. Are students getting adequate education in this area? If not, this leaves them ill-prepared for the needs of the workplace.

The security of our information systems needs to be a major concern for educators and corporate leaders. We recommend that instruction in security and assurance be a core component of the curriculum for all IS and business students. The purpose of this special issue is to provide insights, ideas, and practical tips from IS educators and professionals.

Along with the academic papers in this issue, a new section was added, advisory from professionals. Just as a university information systems department has an advisory board of professionals, this new section provides an advisory to academics; professionals provide insights into the corporate world and they need.

Keywords: Security, Curriculum design & development, Information assurance and security, Computer security

1. INTRODUCTION: NEED FOR INFORMATION SECURITY AND ASSURANCE

> *"America must also face the rapidly growing threat from cyber attacks. Now, we know hackers steal people's identities and infiltrate private e-mails. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."* (Obama, 2013).

Information assurance is an American priority and a global issue. (Information security and assurance includes of data confidentiality, integrity, and availability along with accountability and confidence all is well with the processes.) For example: The United Arab Emirates recognized the need for computer security awareness in higher education (Rezuli and Marks, 2008). South Africa considers education as a critical for information security (Futcher et. al., 2010). Romania, Qatar and the United Kingdom see a need for education on phishing (Al-Hamar, et. al., 2011; Lungu and Tabusca, 2010).

These global security issues are people issues (Rezui and Marks, 2008). And people are the weakest link in security (Kirkpatrick, 2006; Mitnick, 2002). Hence, information security awareness, training, and education of people need to be provided by educational institutions around the globe (Piazza, 2006).

1.1 The value of security and assurance education

While many believe education will lower security breaches and incidents, minimize risks and result in a safer environment (Brown, 1990; Greenberg, 1986; Kirkpatrick, 2006; Kieke, 2006), others have observed that education changes behavior towards preventive or avoidance of misuse (Albrechtsen and Hovden, 2010; D'Arcy et al, 2009; Kruger et. al., 2010). For example, in the 1980's, education and training increased fraud prevention (Brown, 1990). Another example of user weakness is ransomware. Ransomware encrypts user files and then the criminal demands payment to unencrypt the data (Luo and Liao, 2007). Most ransomware infections came from a user's lack of attention to unknown e-mail attachment, or careless browsing and download from a malware embedded Web page (Luo and Liao, 2007). Education is the best countermeasure for these and many other security issues. Given the substantial number of security incidents in organizations, there is a need for more education in the area of computer security. Leach (2003) suggests that the internal threat to computer security is more pressing than external threats and is the "result of poor user security behavior." Goodwin (2005) indicates that IT training is targeted to the CIO, whereas it should be targeted to the "bottom of the pyramid."

Today, most business organizations have installed the latest security hardware and software; however this means nothing if users don't practice cyber safety. Organizations can conduct security awareness training to address policy, procedures, and tools (Peltier, 2005; Rotvoid and Landry, 2007; Ku et. al., 2009). Users must constantly be reminded to be aware of security issues (Peltier, 2005) in order for them to remain proactive and aware of the issues and to minimize the risks (Kirkpatrick, 2006). To get users to "think security" is to create a culture of security (Haber, 2009). To this end, Kabay (2005) made suggestions for enhancing security education and developing a social culture of information security through education.

For most employees, security is not their primary focus. Not all employees can be expected to be security experts nor should they be required to be, but they can be taught to notice suspicious activities, and to alert security professionals when a security-related issue arises (Haber, 2009). There is a need for everyone to learn information security.

1.2 Education problem

Since 1984, user security education, awareness, and training have been important (Dodge, et al., 2007; Schultz, 2004) and stressed by researchers as a method to help reduce the problem (Gage, 1996; Grau, 1984). Unfortunately, the lack of information security awareness is concerning (Mensch and Wilkie, 2011; Okenyi and Owens, 2007). Many colleges and universities lack security education and training in their curriculum (Rotvoid and Landry, 2007); thus it is not surprising that these same colleges and universities have the second highest rate of security incidents (Siegel, 2008). College students practice poor security behaviors and fail to properly use computer security tools (Mensch and Wilkie, 2011). They ignore security issues or simply fail to believe that these information security issues could have major impact their own lives (McQuade, 2007). Educational institutions are the first line of defense (Mensch and Wilkie, 2011) and should provide information security awareness classes (Rezui and Marks, 2008). IS students must gain a critical appreciation the global issues of information security and assurance from their college education**.**

1.3 Need professionals --- a shortage

Along with the need to educate, there is currently a shortage of computer information security professionals for organizations (Bernstein, 2013; Computer Fraud & Security, 2013). According to the Bureau of Labor Statistics, 1.4 million technology-related jobs will be created by the year 2020; however, at current graduation rates, there is expected to be a shortage of more than two-thirds of the IT professionals (Adams 2013). Recently, Enrique Salem, Chief Executive of Symantec Corporation, stated "We don't have enough security professionals and that's a big issue" (Finkle and Randewich, 2012). Other experts are also concerned with the shortage of U.S. computer security professionals (Finkle and Randewich, 2012; ISC2, 2013). According to SANS Institute Research Director Alan Paller, more than 30,000 specialists are needed today. However, he claims that "only about 1,000 to 2,000 have the necessary skills" to combat the numerous real-life scenarios happening in today's organizations (VanDerwerken and Ubell, 2011).

A recent a Booz Allen Hamilton survey found that the nation's cyber defense is seriously challenged by shortages of highly skilled cyber security experts. The report notes that 40 percent of chief information officers, chief information

security officers, and IT managers are unsatisfied with the quality of cyber-security job applicants (VanDerwerken and Ubell, 2011). Tipton, executive director of (ISC)2, indicates that this shortage of skilled cyber security professionals is causing an economic ripple effect across the globe (ISC2, 2013; Computer Fraud & Security, 2013). And listening to the news, it is apparent that no one is unscathed these days.

Cyber security continues to be a top agenda item for CEOs and high-ranking government officials because they know that online security can no longer be partially addressed or uncomfortably ignored (VanDerwerken and Ubell, 2011). As pointed out earlier, educational institutions are the first line of defense with knowledgeable students becoming knowledgeable users in the working world. And more security professionals are needed.

Numerous studies have discussed the importance of reducing computer security risk through giving additional careful attention to computer user security awareness and training but very few papers exist to talk about how to get the content into the curriculum (Gordon, et al. 2005; Aytes and Connolly, 2004; Whitman and Mattord, 2004).

2. TEACHING INFORMATION SECUIRTY AND ASSURANCE AS PART OF THE IS CURRICULUM

Cybercrime embraces all sorts of illegal and ethically questionable activities executed on or facilitated by the Internet, such as impersonation, plagiarism, financial theft, extortion, sabotage, interception, denial-of-service, espionage, fraud, pornography, human trafficking, piracy, hacking/cracking, dissemination of viruses/malware, unsolicited spam, cyberstalking, online defamation, and cyber terrorism (Harris, et al. 2011). But are business school students are getting enough information security training and education to help counter cybercrime?

Today's university graduates will become tomorrow's computer users and security professionals. As such, they will be the protectors of information systems. Therefore, the Department of Homeland Security and the National Security Agency recognize the need to educate a growing number of professionals with a good understanding of information assurance. In order to accomplish this goal, DHS and NSA established the *Committee on National Security Systems (CNSS)* which reviews and designate academic programs as meeting the program requirements. While at least 170 colleges and universities have security programs that have been reviewed and meet the designed program requirements, many other college and universities do not even offer a security class in their information systems curriculum.

While many colleges and universities include an MIS course that is required for all non-computing majors, does that course include a lesson on cyber security and/or ethics? While some of the books offered by publishers for this class include a chapter on ethics, many still do not include a chapter on security.

3. SPECIAL ISSUE OVERVIEW

The study of security and assurance is concerned with issues of data confidentiality, integrity, and availability along with accountability and confidence all is well with the processes. Education is one of the first steps in the process and the purpose of this special issue in the Journal of Information Systems Education. In this special issue of JISE, we have a great selection of articles relating to global information security and assurance in information systems education. The original Call for Papers solicited articles on a wide range of security topics from educators as well as professionals. A new feature titled "Advisory from Professionals" is from Security Professionals currently working in the field. This is an opportunity for professionals from the corporate, government, and military organizations to provide input as to what is going on in their working environments and what is needed from academia. All submissions were double blind peer review in a traditional editorial process. We hope that you will find their view particularly interesting and informative.

IS students must gain a critical appreciation for global information security and assurance from their college education**.** In a survey of over sixteen thousand respondents, sixty-nine (69) percent of organizations indicated that application vulnerabilities their highest security concern; however, most organizations are not addressing this issue (Suby, 2013).

The first paper, a teaching case by Spears and Parrish, could be used to teach students how to securely develop software. (Note: Teaching notes to go along with case are available for verified instructors. Please see http://jise.org/Notes.html for more information.) The case illustrates how UML class diagrams can be used for information classification, data input validation, and regulatory compliance considerations; this case also illustrates how a UML use case diagram can be transformed into a "misuse case" diagram to identify threats and countermeasures; and how a data flow diagram may be used to analyze and document threats and countermeasures to data stores, data flows, processes, and external entities using the STRIDE approach developed by Microsoft. The case is geared toward systems analysts who do not have former training in IS security, and is suitable for upper-division undergraduate or graduate courses.

The second paper demonstrates case-based learning in information security. He, Yuan and Yang share their experiences in using a case study to teach security management. A process model of integrating a case library and Web 2.0 technologies to facilitate case-based learning is also presented in their paper.

The third paper published in this special issue by Patten and Harris provide recommendations for mobile device security education recommendations, which are then mapped to the IT Model Curriculum. The mapping was done using the guidelines from Accreditation Board for Engineering and Technology (ABET). Mobile devices ranked third with 66% of those surveyed indicating it was high on their list of threats and vulnerability concerns (Suby , 2013).

In the fourth paper in this special issue, Ilvonen describes an assignment that she uses in her class to help students bridge the gap between the theory and practice. The students learn how to apply what they have learned in class to identifying security issues in small or medium-sized companies. Course feedback from the students shows that the assignment is perceived to be useful and interesting, and

that it works well when paired with the theoretical teaching of the course. The students find working with real companies motivating, and state that they have learned more than they would have learned on a purely theoretical course.

In order to address the shortage of security professionals, Salem and others have suggested that we need to educate more security professionals (Bernstein, 2013; Computer Fraud & Security, 2013; Finkle and Randewich, 2012; ISC2, 2013). The 5th article in this issue by Woodward, Imboden, and Martin describes how their university added a computer security program to their curriculum.

Along with the academic papers in this issue, a new section was added, advisory from professionals. Just as a university information systems department have an advisory board of professionals, this new section provides an advisory to academics; professionals provide insights into the corporate world and what our corporate partners need from academia. Two of the papers submitted were accepted for this issue including "Preparing Information Systems (IS) Graduates to Meet the Challenges of Global IT Security: Some Suggestions" by Gudigantala and Sauls; and "White Hats Chasing Black Hats: Careers in IT and the Skills Required to Get There" by Fulton, Lawrence, and Clouse. In the first professional advisory, Gudigantala and Sauls recommend that universities addresses the security challenges faced by global organizations by developing the necessary curriculum and includes advice for teaching faculty. The second professional paper is an advisory to universities on twelve subject areas that students should learn if they wish to become a white hat hacker.

4. CONCLUSIONS - CHALLENGE TO IS EDUCATORS

Current university graduates will become tomorrow's protectors of data and systems. It is important for universities to provide training in security and assurance of information systems. Are students getting adequate education in this area? If not, this leaves them ill-prepared for the needs of the workplace.

The security of our information systems needs is a major concern for educators and corporate leaders. We recommend that instruction in security and assurance be a core component of the curriculum for all IS and business students. The purpose of this special issue is to provide insights, ideas, and practical tips from IS educators and professionals.

5. REFERENCES

Adams, P. (2013) Technology talent shortage: Is the solution education, immigration or recruiting women? *Blog:* July 8, 2013. Accessed from http://www.rockiesventureclub.org/2013/07/technology-talent-shortage-is-the-solution-education-immigration-or-recruiting-women/

Al-Hamar, M., Dawson, R. and Al-Hamar, J. (2011). The need for education on phishing: a survey comparison of the UK and Qatar. *Campus-Wide Information Systems*, 28(5), 308-319.

Albrechtsen, E. and Hovden, J. (2010). Improving information security awareness and behavior through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, 29(4), 432.

Aytes, K. and Connolly T. (2004). Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing*. 16(3), 22-40.

Bernstein, C. (2013). IT Skills Shortage: The other critical cliff facing enterprises. *eWeek*, February 2008.

Brown, C.P. (Jan 1990). Crimes of the Vault. *Security Management* 34(1), 31.

Computer Fraud & Security (2013). Study finds major information security skills shortage. *Computer Fraud & Security.* March *2*013(3) 1,3. ISSN 1361-3723, Accessed from http://www.sciencedirect.com/science /article/pii/S136137231370023X on August 1, 2013.

D'Arcy, J., Hovav, A. and Galletta, D. (Mar 2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research* 20(1), 79-98, 155, 157.

Dodge, R. C., Carver, C. and Ferguson, A. (2007). Phishing for user security awareness. *Computers & Security*, 26(1), 73.

Finkle, J. and Randewich, N. (2012). Experts warn of shortage of U.S. cyber pros. *Rueters*, June 13, 2012.

Gage, D. (1996). Companies need more security training programs, study finds. *Info World Canada*, 21(3), 24-25.

Goodwin, B. (2005). Investment in security training on the wrong track, say senior staff. *Computer Weekly*. November 29. 58.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R. (2005). 2005 CSI/FBI computer crime and security survey. *CSI Publications*.

Grau, J. (1984). Security Education: Something to Think About. *Security Management*, 28(10), 24.

Greenberg, M. (1986). Security Awareness + Effective Training = Safer Schools. *Security Management*, 30(8), 47.

Haber, L. (Apr 2009). Security Training 101. *Network World*, 26(16), 30, 32-33.

Harris, A., Yang, M., Yates, D., and Kruck, S. (2011). Incorporating Ethics and Social Responsibility in IS Education, *Journal of Information Systems Education*, 22(3), 183-190.

ISC2 (2013). Shortage of Skilled Cyber Security Professionals Causing Economic Ripple Effect across the Globe, (ISC)²® Study Finds. *PRWEB*, San Francisco, CA. February 25, 2013. Accessed from http://www.prweb.com/releases/2013/2/prweb10464398.htm on August 1, 2013.

Kabay, M.E. (2005). Improving Information Assurance Education Key to Improving Security Management. *Journal of Network and Systems Management*, 13(3), 247-251

Kieke, R. L. (2006). Survey shows high number of organizations suffered security breach in past year. *Journal of Health Care Compliance*, 8(5), 49-50, 67-68.

Kirkpatrick, J. (2006). Protect your business against dangerous information leaks. *Machine Design*, 78(3), 66.

Kruger, H., Drevin, L. and Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security*, 18(5), 316-327.

Ku, C.Y., Chang, Y.W. and Yen, D. D, (2009). National Information Security Policy and its Implementation: A case study in Taiwan. *Telecommunications Policy*, 33(7), 371.

Leach, J. (2003). Improving user security behavior. *Computers and Security*, 22(8), 685-692.

Lungu, I. and Tabusca, A. (2010). Optimizing anti-phishing solutions based on user awareness, education and the use of the latest web security solutions. *Infromatica Economica*, 14(2), 27-36

Luo, X. and Liao, Q. (2007). Awareness Education as the key to Ransomware Prevention. *Information Security Journal*, 16(4), 195-202.

McQuade, S. C., (2007). We must educate young people about cybercrime before they start college. *Chronicle of Higher Education*, 53(18), B29-B31.

Mensch, S. and Wilkie, L. (2011). Information security activities of college students: an exploratory study. *Academy of Information and Management Sciences Journal*, 14(2), 91-116.

Mitnick, K. (2002). The Art of Deception. John Wiley & sons, Hoboken, NJ. (p. 3).

Obama (2013). President State of the Union Speech. http://www.foxnews.com/politics/2013/02/12/transcript-obama-state-union-speech/ (accessed 5/3/13).

Okenyi, P.O. and Owens, T. J., (2007). On the anatomy of human hacking. *Information Systems Security*, 16, 302-314.

Peltier, T. (2005). Implementing an information security awareness program. *EDPACS*, 33(1), 1-18.

Piazza, P. (2006). Security goes to school. *Security Management*, 50(12), 46.

Rezui, Y. and Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, 27(7/8), 241.

Rotvoid, G. and Landry, R. (2007). Status of security awareness in business organizations and colleges of business: an analysis of training and education, policies, and social engineering testing. *Dissertation*, University of North Dakota.

Schultz, E. (2004). Security training and awareness – fitting a square peg in a round hole. *Computers & Security*, 23, 1-2.

Siegel, P.M. (2008). Data breaches in higher education: from concern to action. *EDUCAUSE Review*, 43(1), 72.

Suby, M. (2013) 2013 Global Information Security Workforce Study. *Frost & Sullivan Market Study.* Accessed from https://www.isc2cares.org/uploaded Files/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf on August 1, 2013.

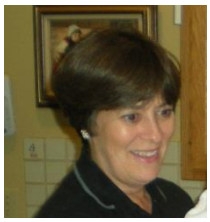
VanDerwerken, J. and Ubell, R. (Jun 2011). Training on the Cyber Security Frontlines. *T + D* 65 (6), 46-50.

Whitman, M. E. and Mattord, H. J. (2004). Making users mindful of IT security. *Security Management*. 48(11).

AUTHOR BIOGRAPHIES

Garry L. White is an Associate Professor in the Computer Information Systems department at Texas State University in San Marcos, Texas. He holds a MS in Computer Sciences from Texas A & M University – Corpus Christi and a PhD in Information Systems Education, from The University of Texas at Austin. Professional Certifications from the Institute of Certified Computer Professionals (ICCP) include C.D.P, C.C.P., C.S.P. and Expert Certified in Security Systems. He also holds the Certified Information Systems Security Professional (CISSP). He has been on the Texas State University faculty since 1997. His research interests and work are in the areas of computer education, human factors with computer technology, infrastructure security, Internet security, privacy, and global assurance. He has published papers in journals such as the Journal of Computer Information Systems and Journal of Information Systems Education. Currently, he is a guest editor for a special issue of the Journal of Information Systems Education; Global Information Security and Assurance in IS Education.

Barbara Hewitt is an Assistant Professor in the Computer Information Systems department at Texas A&M University-San Antonio in San Antonio, Texas. She holds a MBA from Texas State University and a PhD in Information Technology from The University of Texas at San Antonio. Her research interests and work are in the areas of computer security, electronic health records, enterprise resource planning systems, as well as team dynamics during system development. Her papers are published in journals including the Journal of Information Privacy and Security, International Journal of Healthcare Technology and Management, and DATABASE. Currently, she is a guest co-editor for a special issue of the Journal of Information Systems Education; Global Information Security and Assurance in IS Education.



S. E. Kruck is a Professor of Computer Information Systems and Management Science at James Madison University. Dr. Kruck received her BBA in Accounting and Computer Information Systems and her MBA from James Madison University. She went on to complete doctoral studies and earn her Ph.D. in Accounting and Information Systems from Virginia Polytechnic Institute and State University. Dr. Kruck was selected as the Madison Scholar for the College of Business in 2006, the JMU Distinguished Faculty Award in 2007, one of the JMU Be the Change World Changers in 2008, and the Accenture Professional Service Awards in

2011. For the last 5 years, she helped coach and traveled with students to the Association for Information Technology Professionals (AITP) National Collegiate Conference. For 3 years she was part of the Center for Faculty Innovation as a TAP program manager, the Faculty Associate for the Madison Teaching Fellows for both Online Teaching and Part-time faculty. Her research interests include: spreadsheet data quality, end-user computing and education, student motivation and performance, course design and curriculum issues, computer security, and social and ethical issues in information technology. Dr. Kruck is the Editor-in-Chief for *Journal of Information Systems Education*. She has published in the *Journal of End User Computing; College Teaching; Journal of Marketing Education; Information Management and Computer Security; Journal of Virtual Worlds; Journal of Accounting Education; International Journal of Information Security and Privacy*; among others. Dr. Kruck is also a CPA in the state of Virginia.

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 1055-3096