Proceedings of the 11th Colloquium for Information Systems Security Education
Boston University
Boston, MA June 4-7, 2007

An Information Security Course: A Possible Antidote to Clueless Students

Patricia Y. Logan, *Marshall University Graduate College*

Abstract –This paper proposes the inclusion of a required course in information security for university students. College students possess an array of computer hardware, the ability to use Internet resources, and the savvy to find any music, movie, or game online but are ignorant about the fundamentals of information security. Often student computing behavior is reckless and exposes them, their data, and the university network to damage or legal liability. Information security professionals know the value of awareness, training, and education in information security. Awareness programs have not been successful in informing students about the risks they face online and the consequences of their computing behaviors. Knowledge can mitigate or prevent data loss and the impacts of malicious or inadvertent activity. Requiring an information security course can change student behavior, give them the ability to analyze risks, and select the correct tools to protect their data and computers. Information security represents the new computer literacy.

Index terms – Information security, computer literacy, education, and training

I. INTRODUCTION

Literacy has always been at the heart of the education enterprise. From the time of the 3Rs to now, being literate has been a consistent yet evolving foundation for citizenship in each cultural era [1].

With the introduction of affordable personal computers (PCs) and personal productivity software (Microsoft Office) college educators began promoting courses in computer literacy. Advocates for including computer literacy in the general education curriculum believed that teaching basic computing fundamentals was a necessary pre-requisite to school and future employment success in a world moving toward ubiquitous computing. In the 1990s computer literacy became a requirement for undergraduate college students.

Marshall University Graduate College
College of Information Technology and Engineering
South Charleston, West Virginia

Courses were designed and taught by computer information systems or computer science departments that stressed learning the terminology of computing, how computers and media work, teaching light-weight programming, and improving productivity using the MS Office suite. As the Internet was introduced and became a primary source of information retrieval, the computer literacy courses adapted and included content on how to use email and search engines. Librarians added a course (or content) to computer literacy: information literacy. They believed that students needed to learn the mechanics of information retrieval from the Internet, use of search tools, and how to assess the value of Internet-retrieved sources.

Today, the computer literacy course is often waived when students successfully challenge the content by exam or provide evidence of completion of a similar course in high school. Universities that still offer the course are trying to reach those few students without MS Office or information retrieval skills. While students entering college a decade ago may not have had command of computer technology, today's students can comfortably check their email, look up friends in Facebook, rip a CD, and use the copy and paste functions of MS WORD for their term papers. Students can afford their own laptops and use the university-provided wireless access instead of using the campus computer labs. This generation of students has a level of comfort with computing technology that makes the traditional computer literacy course seem obsolete. As a result, some schools have abandoned the computer literacy requirement. Can we conclude that our students are now computer/information literate? Does the possession of a laptop with a wireless connection and the ability to access YouTube and MySpace equate to computer literacy? Should our definition of literacy expand to include the ability to use our computers ethically and securely with full knowledge of how to protect

data and privacy? Based on student behavior, the missing element in computer literacy appears to be information security. Is it time to refocus on information security instead of computer literacy?

Information security touches most areas of our student's lives as they use their computers for most of their class work and literally live "online" with friends, family, and teachers. We should recognize that the content knowledge within an information security course has become necessary to effective citizenship and personal security. Information security skills may need to be taught in a required general education course, and become the "new" computer literacy or at the very least become a well-defined module within a computer literacy course.

Security and privacy have become pervasive issues and this may be the time to reintroduce computer literacy as information security. As educators with discipline-specific expertise in information security, we should be proposing to our schools that all students be required to take a course in information security. Universities have mistaken technical proficiency for an understanding of security. Individuals must ultimately be responsible for their own security practices and protection of their data and our students do not possess these skills. Managing their own security, both while on campus and as employees requires formal education. In the next section, the author will explore what compelling need exists for this course proposal, the appropriate content for such a general education course, and the potential benefits from it being offered.

II. STUDENTS: THE WEAKEST LINK

The last few years have been hard ones for campus information security professionals. In the past three years, computer security incidents at higher education institutions have increased with a number of high-profile "hacks" into university information systems by student intruders [2]. According to California's Office of Privacy Protection, 28 percent of that state's security breaches since 2003 have taken place at a college or university [3]. Student hackers at the University of Texas show the high-profile nature of data loss when students have access to university networks [4]. The security incidents that hit the national press are the tip of a larger problem as many more incidents go unreported such as compromises to student elections, attempts at grade changes, WebCT hacks, and inadvertent malware infections started by a combination of weak security and clueless students. Students encounter their share of grief, too. The recording industry (Recording Industry Association of America) attempts at legal prosecution of college students who illegally download music is a significant concern. In March of this year (2007) RIAA went after a number of universities with pre-litigation subpoenas requiring that universities reveal the names of students that had downloaded music and video from web sources [5]. Students receive volumes of spam on their email accounts (both school and personal) that tempt them into downloading malicious content, giving away personal information or unwittingly participating in an online scam. Some students use the Internet in ways that expose them to harassment, abuse, and possible crime, and others use it in ways that are self-destructive or will compromise future job prospects. The author has had students impacted by information security: stolen laptops with critical work (the 21st century variation on the dog ate my homework), stolen identities, online harassment, scammed via email, downloaded viruses from questionable websites, embarrassed by a post on a personal blog or MySpace entry. Despite the threat of campus computing services removing their account and network access, or being served a warrant for a computer search, students remain naïve and uninformed.

Our obligation as educators is to give students the information they need to thrive in this technological environment and to make decisions as citizens about the use of technology that impact security and privacy (such as electronic voting). Computing isn't simple anymore. Students have a surprising amount of misunderstanding and innocence about security and online activities. Most students cannot configure a firewall and proudly boast that they've never had to install anti-virus (AV) products because they've never had a problem. They naively visit web sites that infect their machines and spread to campus networks. They believe they are anonymous on the web and their

downloading behavior goes unnoticed. They share personal information on YouTube and Facebook that should be private and mis-assess the risk of connections with those they meet online. They are unaware of laws (and penalties) concerning malicious or prohibited activities. In other words, their knowledge of computing is no better than their parents. In most universities there is no course venue for discussion of computing behaviors and the social and technical aspects of information storage and use. This leaves students free to formulate their own ideas about security. But, what are the best alternatives to remedy student ignorance? Are there any venues to provide information security information to college students?

III. HOW DO STUDENTS LEARN INFORMATION SECURITY?

University administrators have taken goal-specific approaches and targeted specific student behaviors that compromise security. For example, to deter student downloading behavior the author's university is proposing fining students when caught by RIAA for the time to investigate RIAA complaints. Some schools limit bandwidth (the "throttle down" approach) to discourage downloads while others filter download traffic targeting file types. Schools offer CDs and university-sponsored web pages with security information and links to free downloads in order to encourage students to install a firewall and anti-virus tools. The author's university provides entering freshman with a CD containing the university AUPs and free AV and firewall tools during freshman orientation and asks students to review the contents prior to logging on to the campus network. Other schools have hosted poster campaigns, video contests, placed articles in student newspapers, sent email messages, offered short courses on security topics, and organized orientation presentations [6]. All of these activities could be categorized as awareness programs. Awareness involves guiding and motivating people on appropriate behaviors. On the continuum of knowledge, awareness is the lowest level, followed by training, and then education. Training helps people develop specific skills. Education provides a broad basis by explaining conceptual frameworks and factual information. Awareness and training are not education. Education is measured by tenure: a day spent in a seminar, a semester in a course, or four years in college. Training, on the other hand, is measured by what can you do when you've completed it. Awareness provides recognition, without deep knowledge or a framework for the application of the information. The National Institute of Standards and Technology (NIST) 800-50 standard summarizes the importance of education in information security: *"The 'Education' level integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge, adds a multidisciplinary study of concepts, issues, and principles (technological and social).."* [7].
The notion of security literacy through training and education has become part of corporate and government efforts to prepare employees to deal with the issues of handling and retrieving data, privacy regulatory requirements surrounding the use of data, as well as computing issues, such as phishing, spam, and the acceptable use of company networks. The federal government has standards (800-series) that require a comprehensive coverage of data security. Public Law 100-235 titled, "The Computer Security Act of 1987," mandated the National Institute of Standards and Technology (NIST) and Office of Personnel Management (OPM) to create guidance on computer security awareness and training based on functional organizational roles. Guidance was produced in the form of NIST Special Publication 800-16 titled, "Information Technology Security Training Requirements: A Role- and Performance-Based Model." The learning continuum modeled in this guidance provides the relationship between awareness, training, and education [8]. In October 2003, NIST also published Special Publication 800-50 "Building an Information Technology Security Awareness and Training Program" [7]. Would such training/education work for a college student population?

Research conducted at Marshall University in 2004-2005 attempted to determine the amount of security awareness of students and whether it impacted risky downloading behavior [9]. Marshall University students are made "aware" of information security through the following: students receive a CD at freshman orientation , sign a statement that they have read the

university Acceptable Use Policy (AUP) prior to network access, and are required to have an anti-virus (AV) tool installed on their personal computer before using the wireless network in the dorm. Students were surveyed in a variety of university undergraduate and graduate classes on the main campus (Huntington, West Virginia). Ph.D. and medical school students were excluded from the study. A sample of 850 students were surveyed in classes from the 13,000 students attending Marshall University. Students were asked if they had read the university AUP, which is required to be signed prior to the issuance of a network identification. The results found that 63% had not read the document and were unaware of any limits on their network use. The survey found that 15% allowed someone else to use their login credentials, an action that would (if discovered) subject students to immediate removal of their network access. And given that Marshall University recently made the top 25 list [10] of most illegal downloads published by RIAA, it is not surprising that 70% agreed that they are downloading music from unauthorized sources [9]. This research follows the author's anecdotal experience with both undergraduate and graduate students in computer science and has found that most students, while proficient programmers and gamers, are unaware of computer laws, how the university (and RIAA) can identify their downloading behavior, and believe any software they download should be legal. Most students have no firewall or AV programs running (despite a university requirement that their computers use these tools if connecting to the university network) and claim confidently that they've "never been hacked." Even the most tech-savvy students were unaware that many downloads from questionable P2P (Peer-to-Peer) sources turn-off the Windows Firewall and leave it off until they saw it happen.

As information systems and security professionals, we believe in training and awareness as critical factors in securing an enterprise. Major security-based conferences, such as NetSec have entire tracks on security awareness and training for corporate employees, who are generally clueless (similar to students) about information security. Any plan for implementing corporate security should include a training component, with the goal of improving security through knowledge. If corporate and government entities believe education produces more informed employees and a more secure network, then can universities not make the same claim for students? Can a course in information security improve university and personal security? Would a course that educates students reduce the number of malware attacks, intrusions, and other information security threats to the university environment? Does training/education work to improve computing behaviors by providing information on how to behave in a high-risk environment? While all training has a short-term impact, it can provide the potential for remediating and changing behaviors with the goal of making students more aware of security threats, their personal information more secure, and making the university's resources safer.

IV. A REQUIRED COURSE IN INFORMATION SECURITY

Information security as a required course can provide insight and understanding about information security, along with technology skills, that can lead to improvement in student computing behaviors and a more secure university network. Information security is at the center of computing behavior, business, the use of technology, and many crimes. Student sophistication and knowledge of the subject area would be an important asset to one's future career. It can improve computing behaviors, make for more cautious consumers, and inform students about the legal constraints on privacy and handling of personal data. A course can provide a venue for the discussion of computing ethics and technology law that does not exist in the present general education curriculum. An information security course would be a good complement to information literacy courses run by librarians, as many issues can be reinforced, such as plagiarism and copyright issues. As the United States government aggressively pursues new initiatives in security, students will need to evaluate and understand the concept of risk assessment and management. Would even our disaster planning be better if it is understood how to assess risk better? Would students (as citizens) be better able to evaluate the security risks inherent in electronic voting or the privacy considerations of legislation that allows

government surveillance of our electronic communications?

This proposal would not duplicate our existing undergraduate information security courses for majors. The focus of the course should be on being able to think critically about how they are using their computer, how to configure their computers for safe computing, how data is stored, evaluating risk, and the best means to secure their computers The parameters for offering this course would be: (1) taught as a required general education; (2) offered early in a student's enrollment; (3) would replace the traditional computer literacy course; and (4) be taught by faculty with information security expertise. The following topics would be components of this course:

a. Why care about information security
b. Configuring a computer for secure computing
c. Trends in surveillance
d. Network attacks
e. Patching software
f. Backup of data
g. Creating passwords
h. Destroying data
i. Network monitoring
j. PKI and certificates
k. Malware
l. Archiving data
m. What does a copyright mean
n. Laws governing technology
o. Criminal behavior
p. Privacy laws (access to data –ISPs for example)
q. Security triad
r. Encryption
s. Security tools (AV, firewall, data recovery, disk wiping, encryption)
t. Layered security
u. Spyware and adware
v. Browser security
w. Social engineering

The design of the course differs from that offered to information security majors in that it would not include the details of malware and malicious activity and not require a strong technical background in computing (or networks) to understand the concepts. Many topics taught in the traditional computer literacy course would still be appropriate for this proposed course. Examples include discussions of how Windows operates, the role of operating systems, file types and structure, and finding information on the web. An attractive side-benefit to this proposed course is that it may also serve as a low-cost recruitment method for students that become interested in the subject and want a career in information security.

Offering a course in information security would target the areas of knowledge weakness that place students in the position of vulnerability. Awareness campaigns only tell students a problem may exist and to be careful "out there". Without instruction, reinforcement, and the ability to develop critical thinking skills about their actions and the context for the arrival of potential threats students will continue to place themselves, their data and the university network at risk.

V. CONCLUSION

Students are often at the center of security issues at universities. From student arrests for hacking into university servers, changing grades in WebCT, to downloading copyrighted material (music, movies, games), to the more mundane issue of plagiarism from web-based sources, student behavior exhibits ignorance about information security. The routine online activities of college students often compromise university computing resources and data stores. Students represent the ultimate insider threat: they have access to a secure network from inside and are end-users without education in secure computing [11]. Students are not getting the information they need to prevent "bad things from happening" to their computer and data. There is no other place in the university general education curriculum for this content. In the absence of knowledge about information security, students will substitute their own ideas (and those of their peers) for correct behavior. A required course in information security may improve the behavior of students and reduce student-related university incidents. We should take the lead in proposing a required course in information security and urge the reformulation of the concept of computer literacy on the college campus to mean information security.

REFERENCES

[1] Serim, F. (2006, October). The Importance of Contemporary Literacy in the Digital Age: A Response to Digital Transformation: A Framework for Information Communication Technologies (ICT) Literacy. *The Big6*. Retrieved March 21, 2007 from www.big6.com/showarticle.php?id=157.

[2] Doan, L. (2006, May). College Door Ajar for Online Criminals. *Los Angeles Times*. Retrieved March 19, 2007, from http://www.uh.edu/ednews/2006/latimes/200605/20060530hackers.html

[3] Zeller, T. (2005, April). Some Colleges Falling Short in Security of Computers. *New York Times*. Retrieved March 6, 2007, from http://web.mit.edu/21w.784/www/BD%20Supplementals/Materials/Unit%20Two/Security%20Privacy%20Identity/universities%20and%20security%20NYT.html

[4] Roberts, P. (2003, March). UT Austin Hacks Yield Info on Thousands. *Computerworld*. Retrieved March 19, 2007, from http://www.computerworld.com/securitytopics/security/holes/story/0,10801,79102,00.html

[5] Mann, J. (2007, February). RIAA Targets Universities for Illegal Downloading. *TechSpot*. Retrieved February 23, 2007 from http://www.techspot.com/news/24438-riaa-targets-universities-for-illegal-downloading-complaints.html

[6]Educause Security Awareness. Retrieved February 22, 2007 from http://www.educause.edu/Browse/645?PARENT_ID=639

[7] Wilson M, & Hash, J. (2003, October). Building an Information Technology Security Awareness and Training Program. *NIST Special Publication 800-50*. Retrieved March 1, 2007 from http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

[8] Wilson, M. (Ed). (1998, April). Information Technology Security Training Requirements: A Role- and Performance-Based Model. *NIST Special Publication 800-16*. Retrieved March 1, 2007 from http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf

[9] Jia, Y. R. (2005, December). "The Impact of the University's Acceptable Use Policy on Student Attitudes Toward Downloading", unpublished [M.S.] Thesis, College of Information technology and Engineering. Marshall University. Huntington, West Virginia

[10] McElroy, J. (2007, March). Marshall Students Could Owe Hundreds of Thousands in RIAA Suit. Herald Dispatch. Retrieved March 2, 2007 from http://www.herald-dispatch.com/apps/pbcs.dll/article?AID=/20070302/NEWS01/703020385/1005/NEWS10

[11] Payne, S. (2003). Developing Security Awareness and Training Programs, *Educause Quarterly*. Retrieved April 22, 2007 from http://www.educause.edu/ir/library/pdf/EQM0347.pdf