Proceedings of the 10th Colloquium for Information Systems Security Education
University of Maryland, University College
Adelphi, MD June 5-8, 2006

Improving Outreach to Adult-Learners Through Online Degree Programs in Information Security: If You Build It, Will They Come?

Patricia Y. Logan Ph.D., Marshall University

Abstract--Traditional face-to-face courses have been used as the predominant delivery mode for degree programs in the area of information security. This mode of delivery is a barrier to information security education for the population of adult learners who are working information technology and law enforcement professionals. Participation in full distance learning programs has been minimal among the CAEIAE (Center of Excellence in Information Assurance Education) schools. An increase in online degree programs can increase the number of degree-qualified professionals in information security. The goal of this paper is to stimulate information security educators to design online programs that fit the needs of adult-learners using a mode of delivery that promotes convenient, available, and cost-effective learning. This paper explores the challenges in providing an effective online program of study in information security and asks the question: Why are there so few online information security programs offered by CAEIAE schools?

Index terms – Information security education, online learning, distance education

I. INTRODUCTION

The growth of online learning has been phenomenal. Estimates from the U.S. Department of Education's National Center for Education Statistics (NCES) provide a best-case scenario of enrollment that projects up to 300,000 new postsecondary students added each year with online (distance education) learning as a principal driving force in this growth [1]. The NCES projected annual growth rates for the comparable period (2003 to 2004) range from a low of 0.87% to a high of 1.31% [2]. The

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

number of students taking at least one online course is now over two million, with over 2.3 million total students in Fall 2004. Overall online enrollment increased from 1,971,397 in Fall 2003 to 2,329,783 for Fall 2004 [3]. This increase in online student enrollment represents a growth of 18.2% and has surpassed the projections made by NCES [3].

Online programs are a key long-term strategy of for-profit schools to appeal to adult learners. Online learning has been one of the reasons for the increase in enrollment of for-profit schools such as the University of Phoenix, DeVry/Keller, Capella, Kaplan, Jones International, and Walden [4]. Online learning has a particular appeal to adult learners in three primary areas: convenience, course availability, and cost-effectiveness [4]. Adult-learners, in contrast to traditional students, do not want to be constrained by a set schedule for attendance, often live and/or work at a distance from a local university, and want to accelerate their learning to graduate quickly. [5] In contrast, online programs are not generally part of traditional university growth strategies, especially at selective or research-focused universities [2]. Laura Palmer Noone, President of the University of Phoenix, summarizes the difference: "Historically, higher education has taken a one-size-fits-all mentality: That if you want to get a degree, you must leave town, stop working, live in a dorm. But we are way past that. We have to be engaged in lifelong learning, especially if our society is to compete globally." [5] Perhaps, threatened by the number of potential students that have moved to online learning programs offered by for-profit schools, over sixty percent

of the traditional "brick and mortar" schools now also offer graduate and undergraduate courses online [3] [5].

Information security has also benefited from the movement to online learning via distance education degree programs. For-profit schools have enthusiastically jumped into the arena of information security degree programs recognizing the growth-potential in an area with a large number of available, high-paying jobs (see http://www.csoonline.com/jobs/index.cfm). The degree programs offered by for-profit schools are designed to be appealing to the population of adult-learners seeking an information security degree using LMS (Learning Management Systems) that provide organization and content displayed for ease of use and 24/7 availability. Courses are offered in an asynchronous mode that does not require students to be in attendance at a specified time. In contrast, non-profit schools have resisted an entirely online information security program. An online search using Google with the search phrase "online degree programs in information security" found seven "brick and mortar schools" (also designated CAEAIE) listed among the more numerous "for profit" schools. Further investigation of these seven CAEIAE school's web sites found that all offered an online graduate degree in information security and none offered an undergraduate degree (one had a degree program in CIS with a concentration available in information security topics). The absence of a complete online degree at these leading purveyors of information security content at the undergraduate level is perplexing. Why are there so few online information security programs offered by the premier providers (CAEAIE) of information security education?

II. CAEIAE AND ONLINE INFORMATION SECURITY EDUCATION

One of the criteria for a successful application for CAEIAE status is to offer evidence of participation in distance education both to improve outreach and student diversity (see criteria at http://www.nsa.gov/ia/academia/caeiae.cfm). The author reviewed all CAEIAE-designated school web sites in order to determine whether they offered a "complete" degree program in information security via an online undergraduate or graduate course of study. A complete information security program is defined as an entire course of study (undergraduate or graduate) resulting in the granting of a degree, that can be completed at a distance with no required physical attendance in a classroom. The author reviewed the Information Assurance web sites provided to (and linked from) the NSACSS (National Security Agency Central Security Service). Few schools had listed enough information to assess from these sites whether online programs in information security existed at the school. Secondary searches using the official school web site were conducted. (Online courses and degree programs for information security were not found consistently in one place making it difficult to determine whether a complete online degree program existed). The author reviewed the appropriate department web sites for evidence of an online program and then reviewed the Spring 2006 class schedule for courses that were listed as having some form of asynchronous learning: either a web site notation (i.e., WebCT) or comment that it was a distance education course. Each university web site was also searched for the presence of an online infrastructure through an organized distance education program that used an LMS.

All schools appeared to offer at least a course in information security available via some mode of distance education. These methods include: videolink, WebCT/Blackboard LMS, web pages, and hybrid (on-campus and distance). Most online courses appeared to be offered asynchronously that students did not have to "attend" a class, lab, or campus site in order to complete the course. A few courses were offered synchronously that required students to visit a satellite campus equipped with a videolink connection to the main campus. (Videolink courses use a dedicated connection between a satellite and main campus classrooms to deliver "live" content). Of the 63 schools with CAEIAE designations (excluding military academies), approximately 15 had an online degree program in information security (23%) at either the undergraduate or graduate level. All of these with two exceptions, were graduate level programs leading to a masters degree. Most schools favored the asynchronous mode of delivery with videolinked courses and recorded lectures popular formats. All CAEIAE schools had an LMS infrastructure in place for the

delivery of online courses (the majority used either WebCT or Blackboard with a few using proprietary systems). The conclusion is that the majority of schools have largely rejected online degree programs in information security, and as a consequence, the adult learner. Why do so few schools offer an online degree program in information security?

The Sloan Consortium in November 2005, released a report on the state of online learning. The response to the question on the value of online education by faculty respondents revealed that there has been little change in the percent of faculty that have a positive view of online learning. The level of perceived acceptance has remained relatively stable since 2003 (28% in 2003 compared with 31% in 2005). [3] The number of faculty with a neutral view of online learning has changed slightly (65% were neutral in 2003 vs. 59% in 2005). [3] There are generic explanations about the reluctance to offer online degree programs (of any discipline) at traditional universities. Among the reasons noted were beliefs that students: do better with a "live" instructor; learn less from online learning; and are less qualified to pursue a degree program [6]. Recent research has dispelled the idea that online education provides a lesser experience with studies that have shown higher levels of student satisfaction and that students score up to 20% higher than students in traditional course offerings [6].

Are there aspects of information security programs that would make faculty reluctant to develop an online program? There has not been research into the reasons information security programs are not entirely online. Possible reasons might include a perception that adult-learners are not likely candidates for an online degree in information security; the cost of developing and managing virtual labs; reluctance to develop an online course without additional compensation; copyright issues with material; or disinterest in increasing an already over-subscribed area of study.

It is known that adult-learners may be years out from their last educational experience but are not less-qualified in terms of their ability to do the work required to earn a degree. Many of these adult-learners are employed in some IT capacity (often in information security), possess recognized industry certifications (i.e., MCSE, CISSP, CISA, CCIE), have completed most of their general education courses, demand courses that reflect "real world" skills, and are focused on earning the final certification: a degree (either undergraduate or graduate) in information security. It is important for CAEIAE schools to understand that these students are exactly the population that should be reached by information security programs—employed in the area, technically-skilled, possessing technical prowess, and have the ability to benefit immediately from the skills. The mandate of NSACSS is to increase the numbers of trained information security workers through the screening and selection of outstanding schools that offer information security degree programs. The large population of working IT professionals and active law enforcement officers should be able to find both undergraduate and graduate degree programs in information security from more than a few sources.

III. THE BENEFITS OF AN ONLINE LEARNING PROGRAM IN INFORMATION SECURITY

The benefits of offering information security degree programs online fall into three areas: an increase in under-represented student populations; outreach beyond the local/regional recruiting area; and capture of adult learners that are working IT or law enforcement professionals.

Increasing the number of under-represented students should be a priority for each CAEIAE. It is a part of the evaluation criteria for the scholarship for service and capacity building grants sponsored by the NSF (see http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5228&org=NSF&from=fund). The demographics of adult-learners would support online learning as a prime means of outreach to under-represented populations. The majority of online learners are women (68% according to research compiled by Noel-Levitz) [4]. The literature (see the NSF study Women in Computer Science by Nancy Leveson, 1989) supports the difficulty of recruiting young women in technical courses of study [7]. Women are under-represented in nearly every information security degree program. While women may have been discouraged from a career in computer science during their

schooling, the female adult-learner is likely to be employed in a computer-related career and eager to complete a degree for career mobility or promotion [8]. An online degree program would significantly increase the number of women in the security pipeline. Additionally, the numbers of under-represented minority populations gravitate to online learning with 12% African-American and 4% Hispanic students currently enrolled in online programs [4]. For-profit schools target Hispanic students with radio and television advertisements in Spanish increasing their access to this under-served student population. It is not surprising that the top undergraduate computer and information systems degree granting schools for Hispanic and African-American students are for-profit and offer online degrees. [9] UMUC (University of Maryland University College) has been recognized as ranking first nationwide in the June, 2005, Black Issues in Higher Education in granting the largest number of master's degrees to African-Americans (2003-2004) through their commitment to online learning. Nicholas H. Allen, UMUC's interim president in August of 2005 said, "One of the most gratifying results of the effort and resources we've invested in online education has been the extent to which we have lowered the barriers to higher education faced by many working Americans, especially those who are under-represented in our colleges and universities. These rankings demonstrate the power of an open university to change people's career prospects and, indeed, their lives. This is why we do what we do" [10]. Online programs do reach these under-represented students in ways that traditional programs cannot.

The CAEIAE schools are not located in all areas of need for information security workers. There are currently 22 states that do not have a designated CAEIAE school (as of April, 2006). Expanding outreach via distance education can increase the number of students enrolling in information security degree programs. Crafting online information security programs can provide distance learning students with the benefits of a quality program despite their residence in a rural area or where there are no available universities with information security programs. Developing online degree programs in information security will attract a larger number of students that otherwise would have no ready access to a quality information security program. Outreach beyond an institution's geographical region is an important component in the CAEIAE program mission (see http://www.nsa.gov/ia/academia/caeCriteria.cfm?MenuID=10.1.1.2). Traditional undergraduate students at age 18 are not as likely to select information security as an emphasis. Even within the computer science major, educators have noted a disturbing drop in enrollments. Between the fall of 2000 and the fall of 2004, the percentage of computer science majors dropped by 60% and by 2004 was 70% lower than its peak in the early 1980s according to the Higher Education Research Institute at the University of California at Los Angeles [11]. Offering an online degree program would capture the population of qualified adult-learners that would increase the number of students in an area of declining enrollment from traditional student populations.

Education is defined in NIST (National Institute of Standards and Technology) Special Publication 800-16 as follows: "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), and strives to produce IT security specialists and professionals capable of vision and pro-active response" (p. 9-10) [12]. As companies and government have embraced networks and e-commerce, the existing population of IT workers has been asked to manage the security of these critical resources. Often, they are managed by bright but incompletely educated workers [13]. NIST distinguishes between training and education of workers as follows: "...education is a degree program at a college or university. Some people take a course or several courses to develop or enhance their skills in a particular discipline. This is training as opposed to education" [12]. Reports have repeated the need for educating IT workers in information security (http://www.careerjournal.com/salaryhiring/industries/computers/20041118-richmond.html). Targeting law enforcement professionals for information security has also been the subject of a number of reports. Most recently Technical Working Group for Education and Training in Digital Forensics (TWEGDE) released a draft report (Fall, 2004) [14] citing education as a critical need for digital forensic workers in law

enforcement. The students exist to enroll in online degree programs in information security. For profit and vendor training programs have offered courses that are designed to meet limited skill objectives and could be more accurately characterized as training instead of education. CAEIAE schools have developed courses rich in content and infused with the active research of information security faculty. Complete programs best satisfy the need for practitioners in the field. CAEIAE schools have largely resisted reaching out beyond their traditional in-class course format. The benefits of reaching out to this population are real and compelling. Given the benefits of online learning, what information security degree programs should be developed that provide education to adult learners? Are there challenges in designing information security programs that provide the same rigor as traditional lecture-based courses?

IV. BUILDING AN ONLINE PROGRAM IN INFORMATION SECURITY

Successful online degree programs require: skilled faculty, degrees designed to take advantage of the needs of adult-learners, and content adapted to the mode of online delivery.

There is a scarcity of terminal-degree qualified faculty with the skills or work experience in computer forensics and network security. One way to compensate for this scarcity is to offer courses online where faculty can be geographically located anywhere and provide a quality experience for students. Universities with qualified faculty can extend the reach of their faculty by using them to deliver online courses. Faculty actively engaged in research and immersed in the subject area would bring to online students a quality that is not possible in for-profit schools that largely use practitioners without terminal degree qualifications or research experience. Online learning requires faculty with dual skill sets: technical skills and the ability to deliver learning online. Universities have implemented an LMS infrastructure (WebCT and Blackboard) that is shared across all disciplines on a campus and available to any academic department for course delivery. Most universities have a distance education office that offers expertise in the design and delivery of online courses. Teaching online is not easier and goes beyond simply converting a syllabus to display as a web page or converting reading material into .pdf files. Many of the CAEIAE schools examined for this paper used videolink technology and recorded classes for their online degree programs. There were no changes made to the instruction style or course format: these are traditional lectures delivered at the convenience of the student. In the author's experience, adult-learners appreciate interaction with other students in the course. Online courses can offer threaded discussions that allow working adults to contribute their knowledge based on their work experiences. In the author's experience, students are more willing to contribute to asynchronous discussions than to make comments in face-to-face classes. A comment the author has frequently heard from online students is that they dislike online courses without a sense that there is an instructor "behind the scenes." Online learning requires a willingness to be available in the same ways that students work, at odd hours and any day of the week. Especially at competitive schools, adult-learners (older and a number of years from their last educational experience) are intimidated into believing that they could not effectively participate in the program. Working IT professionals are often intimidated by traditional face-to-face programs and online learning correctly designed and facilitated online courses can erase the intimidation factor.

Online degree programs must be designed to facilitate the ways that adult-learners want to learn. They cannot be retrofitted from the classroom experience. Adult learners are not the same as the traditional students that faculty are used to encountering in their classes. Students that have forgone a degree in favor of employment are now working adults in IT with promotions and job mobility at-stake. The demographic indicates that these students are between 25 and 54 years old [4]. University courses are often not offered regularly or have rigid schedules of offerings that can make a student wait for years to graduate. For profit and online schools make a compelling case by shortening the course period (compressing the content) and enrolling year round. Despite a cost per unit that is greater than what a public university charges, students will factor the timeframe to graduate into the equation and select the online route [4].

Convenience is a key component of the decision to use exclusively online learning by adult learners [4]. Fixed course offerings (i.e., TTh from 6-8:20) even if offered in the evening do not accommodate the working adult student. The reality of working IT professionals is that work crisises often preclude regular attendance at a scheduled class; out-of-town travel often prevents effective participation, too. Balancing work and family obligations also can interfere with residency requirements for hybrid courses that expect a fixed (one-two week) time for attendance prior to an online learning component. Implementing an online program with required synchronous components will discourage adult-learners. Even the fixed formats of quarters and semesters makes progress appear slow for a professional that possesses many of the skills but lacks the official degree. Learning style is an often overlooked component of the adult learner—many of these students as young adults share an innate interest in computer technology and have taught themselves how to accomplish most tasks without the formal schooling that others may have required. These students study well independently, enjoy discussion forums, are used to posting technical questions on boards, IM routinely, multi-task, install hardware and software without reading the instructions, and have successfully acquired multiple technical certifications completely through self-study and personal experimentation. These students are not interested in self-study so much as collaborative study and interaction. For graduate students an emphasis on collaboration and community instead of research and theory are what practitioners are oriented toward in looking for graduate programs.

Adult-learners work in an interactive and collaborative work environment and look for that same format in the degree programs that they choose. Most for-profit schools do not offer much innovation in their course delivery due to the constraints of course management with a diverse group of adjuncts that are practitioners and not teachers. CAEIAE schools are not similarly constrained and faculty can stretch themselves by using innovative tools to expand their virtual reach and engender student interest. Some innovations that have been applied to improve the interactive component of online courses in information security include:

a. Use chat tools for "lab time consulting" or virtual office hours
b. Podcasts recorded to deliver weekly updates
c. Student directed and produced videos on security commercials
d. Wimba for audio interaction with slide set lectures
e. Inclusion of video, graphics and sound into PowerPoint slides
f. Discussion that is moderated and interactive (asynchronous)
g. Synchronous tools such as Breeze, Netmeeting. WebEx to deliver "live lectures" or hold discussions similar to seminars

However, one area that needs to be addressed for information security courses to be placed online is the issue of computer lab exercises. Can students in online courses of study access the same computer lab facilities from a distance? Online learning would not be as effective as classroom learning if the hands-on activities are removed. A number of universities have managed to implement successfully virtual computer labs and developed exercises that can be done at a distance in network security and computer forensics. These courses offer a number of virtual delivery challenges. CAEIAE schools are best-suited to provide online programs in this area. They have the computer labs, infrastructure, and faculty expertise. Translating hands-on exercises to the virtual environment will take effort. There is difficulty in designing hands-on exercises that teach the student and reinforce skills without direct faculty supervision. In online education there is the additional dimension of doing this remotely and at the convenience of the student. Students cannot be expected to have access to labs when they are in a distance education program, and equipment costs for hardware and software are prohibitive as a purchase requirement for students. Hands-on exercises will need to be designed differently with an awareness that students will not have a live lab instructor and that detailed instructions don't always provide enough information for students doing an assignment on a home computer with unknown configuration. Cookbook style labs (follow the

numbered steps) can lead to serious and discouraging frustration for the student. There is also the concern of remote access from any part of the world to a secure lab that must be resolved between the faculty and campus computing services. There will always be the specter of a problem with unattended exercises that could cause network problems beyond the secure lab environment. Many university faculty are investigating virtualization as a solution using VMWare, Virtual PC, and OptiNET Guru. Textbooks are increasingly available with tools and exercises that don't require licensing expensive multiple copies of forensic and network tools. Many schools are working on automated tools that can setup labs remotely to help students learn defensive network security. Innovative uses of forensics tools and exercises that can be done remotely with success to assist students in responding to computer crime investigations can also be incorporated. Computer games have been developed that simulate network defense. These games could be used across the Internet to allow students a collaborative and team experience (see CyberCiege at http://cisr.nps.navy.mil/cyberciege/) [16].

If we want to ensure that the population that wants a degree in information security receives more than "training" but receives an education that is challenging, rich, compelling, and continues a student's interest in life-long learning, we should all be reviewing our courses for inclusion in an online program. Students want a complete degree program, not an isolated course that still forces them onto campus to complete the rest of a program. Adult-learners, once an undergraduate course of study is completed, will return for graduate degrees and continuing education and increase enrollments in graduate programs.

V. SUMMARY

The awareness of online learning as a viable option for the delivery of an information security program continues to be low. Even TWEGDE referenced only traditional in-class learning for digital forensics and a single mention of online learning (i.e., webcasts). There was no mention of implementing a quality online degree or certificate program in digital forensics, despite the constraints of the target audience (availability). [11]

CAEIAE schools can request funding (under capacity building grants of NSF) to develop robust online learning programs that capture the richness of the classroom experience and enable students to access computer labs and participate in scenarios of attack from a distance. The formation of consortiums with other regional schools to pool resources and provide an online program would substantially benefit students in areas where access to a quality school offering information security is limited. Many schools already possess the infrastructure and need to adapt it to an audience that is not physically present. Perhaps the trickiest issue is the institutional response—online programs can't just be listed in a course schedule and expect students to find the courses. The adult distance learner will not be located in the regional area—they search for programs online. There needs to be an investment in advertising on search engine sites, as well as the development of "micro sites" for advertising a school program on the Internet as well as ads placed in reading material that appeals to online learners. The author's experience in researching existing degree programs at CAEIAE schools was a difficult exercise. Only seven schools advertised their online degree programs effectively enough to be found by a Google search. Most of the schools that linked from the NSACSS web site did not include information about their online degree programs or courses on the information security web site. If we want adult learners to find our program offerings we must design our web sites for their use.

There are two critical adult-learner populations that are candidates for an online degree program in information security: law enforcement and IT professionals. The goal is to reach students in areas that need information security training. Especially in the areas of network security and computer forensics, there is a serious need to increase national capacity. Many adult-learners want to receive the training and are presently moving toward for-profit schools largely due to the failure of CAEIAE schools to offer competitive alternate programs. CAEIAE schools have the capacity, knowledge, and skill to deliver these specialized courses, fulfilling the mission to reach out beyond a school's regional

delivery area. We can increase the number of graduates, improve the quality of security workers, and meet the need for professionally trained workers by expanding into online degree programs. If we build it—they will come.

VI. REFERENCES

[1] "Online Distance Education Market Update 2005: Growth in the Age of Competition", Eduventures, Sean Gallagher with Basar Poroy, June 2005.
[2] "Projections of Education Statistics to 2013", Institute of Education Sciences, U.S. Department of Education, http://nces.ed.gov/programs/projections/tables/table_A01.asp, accessed April 2006.
[3] "Growing by Degrees: Online Education in the United States", 2005, The Sloan Consortium, I. Elaine Allen, Jeff Seaman, November, 2005.
[4] "National Online Learners Priorities Report", Noel-Levitz, 2005.
[5] "Online Schools Clicking with Students", Greg Botelho, August 13, 2004, http://www.cnn.com/2004/EDUCATION/08/13/b2s.elearning/ , accessed March, 2006.
[6] "Distance Education: Better, Worse, Or As Good As Traditional Education?" Online Journal of Distance Learning Administration, Volume IV, Number IV, Winter 2001, Sheila Tucker, http:\research\CISSE\Distance Education Better, Worse, Or As Good As Traditional Education.htm, accessed March, 2006.
Plan for Information Systems Protection, white house 2000
[15]http://cisr.nps.navy.mil/projects/cyberciege.html
[7] "Women in Computer Science," Dr. Nancy Leveson, December, 1989, http://sunnyday.mit.edu/nsf.pdf , accessed March, 2006.
[8] "Women Shunning a Field Once Seen as Welcoming," Marcella Bombardieri, Boston Globe, December 18, 2005, http://www.boston.com/news/local/massachusetts/articles/2005/12/18/in_computer_science_a_growing_gender_gap/ accessed March 2006.
[9] Black Issues in Higher Education, June 2005.
[10] http://www.umuc.edu/fyionline/august_05/fyionline3.html, accessed March, 2006.
[11] "College Students Continue To Shun Computer Science," Linda Tucci, June 8, 2005, http://searchcio.techtarget.com/originalContent/0,289142,sid19_gci1096260,00.html, accessed March, 2006.
[12] "Building an Information Technology Security Awareness and Training Program", Mark Wilson and Joan Hash, October 2003, NIST Special Publication 800-50.
[13] "Hackers Force Creation Of More IT-Security Jobs", Riva Richmond http://www.careerjournal.com/salaryhiring/industries/computers/20041118-richmond.html, accessed March, 2006.
[14] Technical Working group for Education and Training in Digital Forensics, draft, Fall, 2005. http://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf
Defending America's Cyberspace: National