CREATING AN INFORMATION TECHNOLOGY SECURITY PROGRAM FOR EDUCATORS

Joanne M. Kuzma, University of Worcester, Worcester, UK
Sean Kenney, Hillsborough Community College, Tampa, Florida, USA
Thomas Philippe, St Petersburg College, St Petersburg, Florida, USA

ABSTRACT

Information Technology (IT) Security education has become a critical component to college curriculum within the past few years. Along with developing security courses and degrees, there is a need to train college educators and disseminate the security curriculum and best-practices to other colleges. St. Petersburg College implemented a project entitled Information Technology Security and Education for Educators (ITSCEE) designed to address Priority III of the "National Strategy to Secure Cyberspace", establishment of a "national cyberspace training program." The project was designed to produce three nationally relevant IT Security degree and certificate programs at the associate, advanced technical certificate, and baccalaureate levels. Also, the project was designed to provide training and an opportunity for the Florida Community College Faculty to obtain certification in the IT Security arena to assist their institutions in deploying relevant IT Security degree programs. This paper will describe the evolution of this project, the success in meeting goals, lessons learned and techniques and best practices other colleges may use to enhance their programs.

Keywords**:** *Technology Management, Information Security, Security Education, Curriculum, Security Educators, Florida Community College Faculty*

1. INTRODUCTION

St. Petersburg College (SPC) is a public regional college located in St. Petersburg, Florida, and offers a variety of baccelauriate, associate and certificate programs. Their purpose is to provide degree programs and training to meet local industry and business needs in a variety of educational arenas including Technology Management and Computer Security. SPC continually analyze the current market needs and meets with industry leaders and subject matter experts in recognizing new industry trends and shortages of personnel in key areas. One of these key areas identified is a critical shortage of employees with skills in Security Technology and Management.

1.1 PROJECT EVOLUTION

In 2003, several members of industry met with key SPC officals to address the dire needs for graduates with degrees in Information Security and to identify a program to potentially satisfy industry needs. The proposed program was initially presented to the SPC Board of Advisors in 2003, an a market and needs analysis study was initiated to determine the market potential.

This study was subcontracted to "CEREBIT," a local consulting firm that specializes in information security. They completed a proprietary report entitled "Needs and Market Study for the Bachelor of Applied Science Degree in Security Management." The study surveyed 23 Tampa Bay companies, and all anticipated a strong demand for professionals with a Bachelor's degree in Information Security Management. The study also examined demand outside the Tampa Bay area at the national level and found a similar need for highly educated security professionals across the U.S. Also, currently many jobs are now handled by computer science professionals with specialized security certificates and strong technical skills. However, many firms indicated a need for professionals who have more broad skills in

implementation and management, as well as specific technical training. These skills could be gained in a proposed Bachelor of Applied Science Degree.

The results were presented to the Board in 2004, and they concured there was a need for personnel with specialized security skills. They also determined that information security professionals responsible for meeting the mandates of the US Federal Government regulation, such as Sarbanes-Oxley Act and HIPAA, as well as meeting industry needs will have to have business and management skills as well as technical security knowledge. At this time, it was decided to gradually introduce additional security topics in specific courses and to initiate a full program in 2005-2006.

In October, 2005 the full program was given permission to proceed, and the National Science Foundation (NSF) funded a grant to implement the project (ITSCEE) to advance security education training for community college staff and students.

1.2 PROJECT OBJECTIVES

SPC identified three overall areas of emphasis in developing the program: 1) developing people, 2) developing the analysis and data collection processes, 3) implementing technology into the project. SPC and its education and industry partners then designed a three-tier IT higher-education model comprised of three goals:

1. To develop a nationally relevant curricula for an Associate of Science Degree, an Advanced Technical Certificate, and a Bachelor of Applied Science of Information Technology that integrate widely accepted IT security skill standards and high demand industry certifications from (ISC)² (International Information Systems Security Certification Consortium), NWCET (National Workforce Center for Emerging Technologies), CompTIA (Computer Trade Industry Association), and NSTISSC (National Security Telecommunications and Information Systems Security Committee).
2. To provide faculty development opportunities in information security for the 56 community colleges in Florida to result in preparation for a nationally recognized certification.
3. Disseminate the curriculum and best practice knowledge gained in this project to 1100+ community college in the United States and to selected high schools in Florida to stimulate an interest in IT security careers and to increase the number of students enrolling in and graduating from the IT security programs at community colleges nationwide.

2. LITERATURE REVIEW

The U.S. Department of Labor's Career Guide to Industries states that “demand for computer security specialists will grow as businesses and government continue to invest heavily in cyber security, protecting vital computer networks and electronic infrastructures from attack.” (Bureau of Labor Statistics, 2007-2008) Job prospects are high for college graduates who have formal training as well as related work experience, as the private sector and government has difficulty in finding workers with qualified skills.

After the events of 9-11 and with the increased emphasis on Homeland Security, the U.S. government increased funding for computer security programs and training opportunities. In 2001, the NSF implemented the Federal Cyber Service: Scholarship for Service (SFS) program which seeks to increase the number of students in the IT security field by providing scholarships to qualified college students and also to provide funds to colleges to increase the number of students in computer security programs, and has an anticipated funding of $5,700,000 for fiscal year 2008 (Federal Cyber Service, 2006). The NSF has also provided other grants colleges and universities. In 2005, the NSF awarded a 4-year, $3 million

grant to Anne Arundel Community College in Maryland to develop an Information Security Assurance major (Orchowski, 2005).

Although the emphasis of security training at the college level is often on the technical aspects, it is also important to develop a broad range of skills in or to function more effectively in the business environment. At SPC, students taking the certificate route emphasized the technical security aspects of the program to develop strong technological knowledge. Students enrolled in the AS and BAS degree programs would take a variety of technical, managerial and general education classes in order to develop a broad basis of skills. Other colleges have recognized this need to develop this combination of technical, communications and social-related skills. For example, Dartmouth's Computer Science Department introduces students to security's technical aspects, but also does not neglect the social aspects of education, such as legal aspects, privacy and social engineering (Bratus & Masone, 2007). U.S. Department of Labor's Career Guide to Industries also recognizes that for these technical specialists, strong communication skills as well as analytical skills are important (Bureau of Labor Statistics, 2007-2008).

Developing a strong security program would not be possible without a strong cadre of well-trained security faculty. Because of the rapid change in this field, it is important for faculty to continually enhance their technical knowledge as well as develop relationships with other colleagues and industry professionals. Boggs (2002) recommends several key elements community colleges should implement when support security faculty:

- Continuing education for security faculty to complete certification and remain current.
- Faculty participation in professional organizations.
- Support to for faculty to learn techniques to teach technical classes.
- Help for faculty to develop new courses.

It is important for local colleges and industries to contribute to faculty growth, not only for each individual college, but for a sharing within a group of associated schools. One example of an effective program was Northern Virginia Community College (NVCC). In 2001, they started a community of information security faculty in 23 community colleges in the Virginia area. These faculty worked together to collaborate on curriculum development, knowledge management, faculty training and information sharing (Morneau, 2004).

3. PROJECT IMPLEMENTATION

After the NSF granted was secured, the project was divided into several key phases in order to meet the key deliverables. In October 2005, the project was given permission to proceed, and the main portions of the project were developed after January 2006. The first phase of the project was in developing the overall curriculum. Meetings were held with industry leaders and subject matter experts to analyze the overall curriculum, degree programs and classes to be developed. In the Spring of 2006, course development began and lasted for a year. Concurrently, faculty development and training was instituted. The final project phase was to disseminate the security information and document best practice knowledge gained from the grant process In June 2008, the project was completed.

3.1 DEVELOP A CURRICULUM

The first goal of this grant was to enhance existing curriculum and develop new curriculum in IT Security Degree and Certificate programs for use at community colleges nationwide based upon information security skill standards developed by $(ISC)^2$, NWCET, CompTIA and NSTISSC. This included developing three versions of the degree and certificate programs: a classroom based, an online, and a blended, which is partly online and classroom; enhance the existing AS degree by integrating SSCP® into it, develop the Bachelors of Applied Science degree program in Information Security and Security Management. Because SPC and partner community colleges currently have existing computer security lab facilities that will be used for field-testing curriculum, equipment acquisition was not needed.

This activity put most effort into the intended focus of the creation of three programs: Certificate, Associate level Science Degree (AS), Baccalaureate Science Degree (BAS). These were completed to enable traditional on-ground classroom delivery, online using numerous Internet technologies), and blended (a combination of the previous two approaches).

Campbell & Hawthorne (2002) indicate that the four broad categories that most community colleges offer in cyber-security are:

- A two-year associate degree
- A 1-year institution-granting certificate
- A credit course that is part of an existing program
- A non-credit credential program

Instead of offering student options in all four of these categories, the SPC mandate was to concentrate on offering a two-year associate degree and certificate. Students would also have the option to take a single credit course if spaces were available. A non-credit credential program was not considered. In addition, although SPC was founded in 1927 as a community college, in 2001 Florida approved legislation which made SPC the first community college to award 4-year degrees. They now offer over 20 bachelor degree programs, as well as the community-college level associate degrees and certificates.

By spring of 2007, St. Petersburg College had successfully launched all three tiers of this academic career ladder and finished developing all courses. A list of completed courses is found in Table 1. Courses with the CIS, CGS and CET prefixes were developed for the AS and certificate level programs. Courses with the BUL and ISM prefixes are intended for students taking the BAS degree program. The table also shows the number of times each course has been offered between Fall 2006 and Spring 2008 and the number of students enrolled. The development of both the curricula and the coursework in these programs has been through a rigorous review process including a review by faculty members, industry professionals and the Curriculum and Instruction (C&I) committee of the college.

The relationship with $(ISC)^2$ was forged in this project and built out to culminate in a formal Memorandum of Understanding. The agreement came into effect January, 2008 after both the President of SPC and the Director of $(ISC)^2$ signed it. The fruits of the NSF project were further demonstrated with the $(ISC)^2$ Resource Handbook referring to these new course resources. St. Petersburg College and Seminole Community College form two of 16 sources linked directly from the document.

The courses were developed using all of the currently relevant national standards for information security professionals. This outcome fed into the newly designed courses and a cross-reference mapping to the external standards. The courses and curriculum have been scrutinized to ensure an equitable treatment for women and minorities. The curricula and coursework developed in partnership with industry leaders, SME's, and various faculty mirrors the nationally accepted standards of all of the organizations and government agencies on which the project was to focus. The development of the course materials was reviewed by St. Petersburg College's College of Technology and Management Advisory Board which consists of industry leaders of both local and national organizations. Staffing within the faculty and project members at the operational level indicate a particularly strong result in this regard, including opportunities for academic advancement within this NSF grant.

Faculty that were not previously qualified with the $(ISC)^2$ completed training and examinations where they became CISSP qualified in 2007 through this NSF grant initiative. There will be a particularly strong emphasis for SPC's current and future faculty to have a CISSP.

In addition to the original development of the curriculum SPC remains committed to constant quality improvement of the content for these courses relative to industry and student needs. SPC utilizes a comprehensive evaluation process known as the Student Survey of Instruction (SSI). The SSI is a process which allows students to evaluate the delivery of the course materials, facilities, and faculty. This provides valuable feedback regarding the efficacy and quality of the materials. A further process to

improve content and delivery came from the full set of the Technology Management Board of Advisors (TM-BOA). Faculty reviewed the SSI results, considered the TM-BOA input and reviewed current industry best practices to ensure a relevant and rigorous curriculum.

TABLE 1. COURSES DEVELOPED

Course #		Description	# of Times Offered	Enrollment
CIS	**1354**	Introduction to Network Security	6	61
CIS	**1358**	Operating System Security	4	36
CIS	**1356**	Network Security & Firewalls	3	24
CIS	**1353**	Network Security Audit-attacks/threats	2	11
CIS	**1355**	Security Engineering	1	6
CIS	**1350**	Network Defense & Countermeasures	4	35
CET	**2691**	Laws and Legal Aspects of IT Security	4	31
CIS	**2357**	Database Security	2	13
CGS	**2811**	Incident Response and Disaster Recovery	3	15
BUL	**3564**	Legal Aspects of Managing Technology	4	72
ISM	**3320**	Core Security Principles	2	41
ISM	**3324**	Applications in Info Security	4	74
ISM	**3330**	Info Security Policy Adm & Mgmt	4	48
		Total	43	467

3.2 FACULTY DEVELOPMENT

The second main object for this project was to provide faculty development opportunities in information security for the 56 community colleges in Florida to result in preparation for a nationally recognized certification. This goal was the primary focus for the “Education for Educators” portion of the project. The concept was to provide training and career development opportunities to college faculty. These opportunities would enable them to obtain a professional certification in Information Security which they would be able to utilize in building a curriculum at their own institutions. The focus of this training program centered around a three-tier format that included online self-paced modules, 3 day boot camp preparation, and culminating with a private sitting for the CISSP exam administered by $(ISC)^2$. The iTEC PI facilitated the contact with the 56 community colleges in Florida to garner interest in the training program. The training program was to be (as noted above) an online self-paced study of the 7 domains of the SSCP and the 10 domains of the CISSP that was hosted on SPC’s ANGEL Learning Management system. Upon completion of the 17 online modules faculty were to participate in a 3 day “Boot Camp” session using certified $(ISC)^2$ instructors to review the material prior to the CISSP exam. On the weekend following the 3-Day boot camp, faculty members were provided the opportunity to sit for a private session of the CISSP exam that was proctored by $(ISC)^2$.

Due to shrinking budgets and several other factors, it was learned that several of the Community Colleges in Florida had either eliminated or drastically reduced their Business Technologies disciplines and therefore interest from those institutions in the training was virtually non-existent. As a result of several communications including e-mail, phone follow-up, and brochure distribution there were a total of 25 faculty members from 13 participating institutions that were part of the online portion of the project. Again, due to budget constraints and scheduling issues within the school semester, only 12 of the 25

faculty members were able to attend the boot camp. Of the 12 members involved in the Boot Camp, 6 faculty members completed the examinations.

Given the shrinking budgets, shrinking staff and other factors in the State of Florida Community College system the results here represent a healthy participation in the quest for industry certified professionals to further the Information Security profession. The same budget challenges led to the need for solutions such as the SLIS laboratory. The integration of reasonably priced, industry relevant solutions, will improve student instruction options and enhance the outreach to faculty.

3.3 DISSEMINATE INFORMATION AND BEST PRACTICES

SPC's third major objective was to disseminate the curriculum and best practice knowledge gained in this project to 1100+ community colleges in the United States and to selected high schools in Florida to stimulate interest in IT Security careers and to increase the number of students enrolling in and graduation from the IT security programs at community colleges nationwide.

This goal was divided into two sections: developing the web-based content and then disseminating that information to various colleges. A web-based brochure describing IT security careers, salaries, prerequisite skills and a student career-assessment instrument related to IT Security was created. The ITSCEE website noted earlier (at: http://www.spcollege.edu/itsecurity/itscee/library.htm) has been divided into a number of components including industry information, career information, curriculum and teaching aids. This web site serves as the portal for all information distribution for the project, including all of the activities rendered in the third goal. The materials are available to the relevant parties with the ITSCEE Web site providing the contact point. Not all materials are available for immediate download as many require restricted access. One example would be that students should not use this facility to access courses and tests as this would impinge on proper assessment.

The second phase of the this goal was to distribute web-based brochure via e-mail to 1,100+ community college career centers nationwide and to the selected high school career centers in Florida. The American Association of Community Colleges (AACC) was to provide mail and e-mail addresses for the colleges as well as reference the availability of these new resources in journals, at conferences, in newsletters and on its website.

However, due to budget issues and other personnel related changes on the project team the original resource required to accomplish this task left the project team. Further were attempted through the iTEC links; however, these did not yield results. This resulted in a scope reduction in the NSF grant. An alternative route has been launched to exploit the market to other colleges through educational focus groups in bodies including the IEEE and the ACM.

4. CONTRIBUTIONS TO THE DISCIPLINE

St. Petersburg College has developed and implemented an academic career ladder that includes a Certificate in Information Technology Security; an Associate of Science degree in Information Technology Security; and an Information Security Assurance track in the Bachelor of Applied Science in Technology Management degree. This academic career ladder that is offered as part of the 2-Year/4-Year community college degree program is the first of its kind in Florida. It offers those interested the opportunity to develop the necessary skills to become part of the Information Security profession. This degree program advances the profession of Information Security through its rigorous academic standards integrated from other NSF projects such as iTEC, NWCET, CompTIA, $(ISC)^2$, and NSTISSC IT Security skill standards. Leading practitioners from companies such as CitiGroup, Raytheon, Ditek, Franklin Templeton, Verizon, Tech Data, and Brighthouse provided further insights.

The program core curriculum and course descriptions are available to all community colleges in Florida and the nation through our ITSCEE web site. The fruits of this project have resulted in the execution of 43 courses in security and had 467 student enrollments. This practical experience has already resulted in

improvements and adjustments to enhance the outcome. Enrollment is positive and should improve as marketing activities are implemented. New approaches and solutions to involve more remote faculty promise a better response in this area too.

The ITSCEE project was focused on advancing professionalism and increasing the awareness of Information Security and the Information Security profession. This NSF project did provide a route to improve support for security from Human Resources, Banking, Strategic Management, Management and Leadership disciplines. By garnering support through education and insight, these other areas will provide support and resources to improve security outcomes. Similarly, the new sensitivity and understanding of faculty in these disciplines should propagate to an even broader relevance for sound security objective. Major contributions to human resource development from the project come in the form of the graduates from both of the academic programs offered by St. Petersburg College as well as the "Education for Educators" training that provided professional certification opportunities for 25 Florida Community College faculty members. Graduates from the academic programs will enter the workplace with the necessary skills in Information Technology Security.

The faculty members who participated in the training program have increased their knowledge of the Information Security arena to assist in helping their institutions develop programs to further the profession. In addition, at least 5 of the participants successfully obtained the professional certification of CISSP which will help those faculty members build programs and impart key concepts of the Information Security profession.

5. CONCLUSION

Several key items of interest in the ITSCEE project have been observed leading to improved approaches to ensure the strategic and ongoing successes hoped for in this NSF grant The project initially targeted education of Florida Community College faculty in order to increase the awareness of the Information Security career path and to provide training opportunities for faculty to obtain industry standard IT Security certifications. This project was completed in June 2008, and the process enhanced the learning experience of future Information Security Professionals through developing more highly qualified faculty.

Despite adversity from the economic downturn in the State of Florida, the grant reduction, and shrinking education budgets, the spirit and the practical development contemplated by the NSF grant was accomplished. The scope adjusted due to the grant modifications and the reduced number of Community Colleges in Florida offering Business Technologies disciplines. While this impacted the numbers of linkages, the new approaches contribute to stemming the tide and enable the achievement of better outcomes in difficult economic times.

The delivery team on the project adapted solutions to the adverse financial climate as these impediments occurred, the most recent example being the inclusion of the SLIS laboratory to extend access to practical security solutions through distance techniques. These benefits will accrue not only to students, but also to remote faculty.

The academic career degree ladder initially proposed has been accomplished, the project team was able to share the project materials with a number of institutions, and the Education for Educators goal was able to successfully credential faculty members in the CISSP certification process. The degree programs instituted by the project, as well as the Web site and other materials, will continue well past the project completion given the number of students and institutions interested in this academic career path.

6. REFERENCES

Boggs, G. (2002, June). *The Role of Community Colleges in Cyber-security Education.* Presentation to the workshop sponsored by the AACC and the National Science Foundation. Retrieved June 27, 2008 from

http://www.aacc.nche.edu/Content/NavigationMenu/ResourceCenter/Projects_Partnerships/OtherInitiatives/Cybersecurity/Cyberreport.pdf
Bratus, S. & Masone, C. (2007, November). *Hacker Curriculum: How We Can Use It in Teaching*. IEEE Distributed Systems Online. November 2007. (vol. 8, no. 11), art. no. 0711-mds2007110002.
Bureau of Labor Statistics, U.S. Department of Labor, Occupational Outlook Handbook, 2007-08 Edition, Computer Support Specialists and Systems Administrators. Retrieved June 27, 2008 from http://www.bls.gov/oco/ocos268.htm .
Campbell, R.D. & Hawthorne, E.K., (2002, June). *Cybersecurity Education in Community Colleges Across America: A Survey of Four Approaches by Five Institutions.* Paper presented at the role of community colleges in cybersecurity education: A workshop sponsored by the AACC and the National Science Foundation. Retrieved June 27, 2008 from http://www.aacc.nche.edu/Content/NavigationMenu/ResourceCenter/Projects_Partnerships/OtherInitiatives/Cybersecurity/Cybersec_Ed_in_CCs.pdf
Federal Cyber Service: Scholarship for Service (2006, November). National Science Foundation, http://www.nsf.gov/pubs/2008/nsf08522/nsf08522.htm, Retrieved June 27, 2008.
Morneau, Keith. (2004), *A Community of Information Security Faculty: An Innovative Approach to Continuous Course Development in Community*. Electronic Journal for the Integration of Technology in Education. Vol. 3, No. 3., Fall 2004 . pp. 30-41. Retrieved June 28, 2007 from http://ejite.isu.edu/Volume3No2/Morneau.pdf .
Orchowski, Peggy. (2005, December 19). *NSF Grant Opens Door to Cybersecurity Major in Maryland*. Community College Week. Vol 18 Issue 10, p 3-9, 2p; (AN 19281575).

7. AUTHORS PROFILE

Dr. Joanne M. Kuzma earned her Ph.D. in Information Systems at Nova Southeastern University in Fort Lauderdale Florida in 2006. Currently, she is a full-time faculty member of the Worcester Business School at the University of Worcester, UK.

Sean Kenney earned his M.B.A. at Southern New Hampshire University. Currently he is a full-time faculty member at Hillsborough Community College in Tampa, Florida.

Dr. Thomas Philippe earned his Ph.D. in Engineering at University of South Florida. Currently he is a full-time faculty member in the College of Technology Management at St Petersburg College in St Petersburg, Florida.