Curriculum and Pedagogical Effects of the Creation of a Minor in Cyber Security

Frank H. Katz
Armstrong Atlantic State University
Department of Computer Science and
Information Technology
Savannah, GA 31419
912-344-3192

frank.katz@armstrong.edu

ABSTRACT

In January 2006, Armstrong Atlantic State University(AASU) offered its first course in Information Security. At the same time, the university received funding for its Cyber Security Research Institute, a non-academic unit closely related to and funded by the U.S. Department of Homeland Security. The establishment of this research institute led the administration, the Department of Criminal Justice in the College of Arts and Sciences, and the School of Computing to create an academic minor in Cyber Security to be cross-listed between Criminal Justice and Information Technology. This paper describes the pedagogical effects of the creation of the minor and future implications for it and for the teaching of Information Security at Armstrong Atlantic State University.

Categories and Subject Descriptors

K.3.2 [**Computers and Education**]: Computer and Information Science Education – *curriculum*, *information systems education.*

General Terms

Management, Measurement, Security, Human Factors.

Keywords

Information security, Cyber security, Curriculum, Pedagogy.

1. INTRODUCTION

When the Information Technology major was introduced at AASU in 2002, there was no requirement that students take a course in either Computer or Information Security. Both CS and IT students were required to take a course in Ethical Considerations in Computer Science, which has since been renamed as Introduction to Computer Ethics and Cyber Security. However, there was no course that addressed the growing field of Information Security.

In Fall 2003 it was decided that an IT course be created in Information Security. I volunteered to create a course in this field, and in order to do so, I reviewed the curriculum of several universities that offered the IT major to determine if they had such a course and its contents. Upon discovering Kennesaw State University's (KSU) information security program, I attended a one-day program at KSU on textbook selection. A special topics trial version of the course, ITEC 4990, using the 1st edition of Whitman/Mattord's Principles of Information Security was created during the Spring 2004 semester and taught in the Fall 2004 semester. By the Spring 2006 semester, the course had been approved as a permanent addition to AASU's Information Technology curriculum as ITEC 3100 and was taught again in Fall 2006. It was decided that the new course would only be offered each year during the Fall semester. In December 2006 I attended a three-day workshop at KSU on how to create a course in Information Security or improve an existing InfoSec course. Tips and techniques learned at this workshop were implemented in teaching the course the next time it was offered in Fall 2007.

During the summer of 2007, discussions began between the university's administration, the department of Criminal Justice (CJ) in the College of Arts and Sciences, and the School of Computing to create a Cyber Security minor. One of the goals of creating the minor was to create an interdisciplinary program by offering it to students majoring in Criminal Justice. The results of these discussions were significant changes to the Information Technology curriculum proposed and approved during the Fall 2007 semester.

2. CHANGES AND CHALLENGES TO THE CURRICULUM

The most striking change to the IT curriculum was the request from Criminal Justice to elevate the existing Information Security course from a 3000 to a 5000 level, and to divide it into two new courses. This was based on CJ's desire to offer the minor to students earning a Masters in Criminal Justice and to create a robust minor containing two Cyber Security courses.

At the time, the syllabus of ITEC 3100 followed the material in the Whitman/Mattord text: foundations of information security, policy and procedure development, risk analysis and management, the components of an effective information security plan, encryption, and some technical discussion of firewalls, VPNs, and intrusion detection systems. In effect, the task was to create two courses out of one, and make each more robust than ITEC 3100. The two courses were numbered ITEC 5001, Cyber Security I,

Information Security Curriculum Development Conference 2010, October 1-2, 2010, Kennesaw, GA, USA.

and ITEC 5002, Cyber Security II. As an interdisciplinary program, the minor was to be primarily listed in the catalog as part of CJ, cross-listed with IT. ITEC 5001 and ITEC 5002 would also be cross-listed as CRJU 5001 and CRJU 5002.

The course description for each follows:

> "**ITEC 5001U CYBER SECURITY I**: Current standards and best practice in information assurance and security. Topics include evaluation of security models, risk assessment, threat analysis, security implementation, disaster recovery planning, and security policy formulation and implementation."
>
> "**ITEC 5002U CYBER SECURITY II**: Concepts of countermeasures and safeguards such as remote access controls, firewalls, intrusion detection systems, virtual private networks, and data encryption." [1]

Clearly such a change would require a significantly richer course in the study of more technical security mechanisms such as IDSs and VPNs. For IT students, ITEC 3100 had been a required course from its inception, and ITEC 5001U would replace it as a requirement in the IT course of study. ITEC 5002U would become an elective, and this would have major implications for the future administration of the minor.

Besides the challenge of creating two courses out of one, a minor requires 18 credit hours, or six courses. The question facing the IT and CJ departments was, which courses would comprise the minor? It was determined that in addition to the two new ITEC/CRJU courses, students would take one more CRJU course from:

> **CRJU 3300**: Criminology; **CRJU 3500**: Criminal Evidence and Procedure; **CRJU 3600**: Topics in Criminal Justice; or **CRJU 5500U**: Law and Legal Process. [2]

Courses from the IT curriculum would include:

> **CSCI 1150**: Fundamentals of the Internet and the World Wide Web; **CSCI 2070**: Introduction to Computer Ethics and Cyber Security, which is the pre-requisite for ITEC 5001U; one course from **ITEC 1310**: Programming in Visual Basic, which is the IT pre-requisite for CSCI 2070, or **CSCI 1302**: Advanced Programming Principles, which is the CS pre-requisite for CSCI 2070. [2]

These curriculum changes were approved by the University Curriculum Committee during the Fall 2007 semester. Given that ITEC 5001U is only taught during the fall, and that the pre-requisites for ITEC 5001U were all IT or CS courses, when the Cyber Security minor was approved, it was assumed that it might take one complete academic year before any CJ students registered for ITEC 5001U. So it was assumed that the earliest a CJ student would enroll in ITEC 5001U would be the Fall 2009 semester.

3. IMPLEMENTATION

3.1 Changes to ITEC 3100 to create ITEC 5001U

Changes were necessary to make ITEC 3100 into a graduate-level course. It did include a class or group project. Two cohorts of the class conducted university-wide laptop virus scanning sessions, one of which was previously documented in "Campus-wide Spyware and Virus Removal as Method of Teaching Information Security," presented at this conference in 2006 [3]. Despite the practical nature of having students plan and implement such a project, it was felt that at the graduate-level, they would best be served by enhancing the current course with case-based material. Indeed, "although it is well known that learning is enhanced when theory and practice are integrated, students often have difficulty relating classroom material to the practical working environment." [4] Consisting of a series of real-world case studies focusing on different aspects of information security, the book "helps students to develop the practical understanding needed to cope effectively with the responsibilities of the profession" [4]. Students were required to read various cases as they corresponded to the textbook and write essays on each. In addition, the cases themselves formed the basis of a semester-long project.

In addition, as a 3000-level course, tests had been strictly multiple-choice. With its promotion to a 5000-level course, multiple-choice tests were either dropped or limited to a few questions per test, replaced by paragraph questions.

3.2 ITEC 5001 Enrollment

Although it was presumed that students majoring in CJ would not have the necessary pre-requisites to take ITEC 5001 for at least one full academic year, the need for CJ students to enroll in the course caused CJ faculty to give all three CJ students enrolling in the Fall 2008 cohort prerequisite overrides. Of the nineteen students enrolled in the Fall 2008 section, one was a CJ undergraduate, and two were graduate students. Two of them had not taken any of ITEC 5001's computer science and information technology prerequisites prior to enrolling in the course. One had only taken one of the three CS and IT prerequisites. The Fall 2009 section saw a similar situation: out of the twenty-two students, one was a CJ graduate student and one was a CJ undergraduate. The undergraduate student had met all of the CS and IT prerequisites and the graduate student had met none of them.

3.3 ITEC 5001U Results

The grade results of the two sections that have contained CJ students have to first be evaluated in comparison to the previous sections when ITEC 5001 was ITEC 3100. The three previous sections, Spring 2006, Spring 2007, and Fall 2007 resulted in the following composite grade distribution: 13 A's, 16 B's 4 C's 2 D's, and 1 F.

The two sections of ITEC 5001U were Fall 2008 and Fall 2009. For Fall 2008 they were: 11 A's, 4 B's, 1 C, 1 D, and 1 F. For Fall 2009 they were 7 A's, 9 B's, 3 C's, 1 D, and 2 F's. The grades of the CJ students were significantly lower than those of the IT students. In Fall 2008, the three CJ students earned one D, one B, and one F. Fall 2009's results were worse. The only two CJ students in the class both made F's. The specific test, assignment, case study, and project grades which covered more technical topics such as the basics of encryption, IDSs, firewalls, and VPNs were either not turned in or significantly lower than those of the IT students. The case studies and Test 2 in both years of ITEC 5001 covered technical topics such as firewalls,

VPNs, and IDSs. In 2008, the IT majors scored an average of 84% on the case studies and 87.9% on Test 2, as opposed to the CJ majors, who averaged 70.4% and 53.3% respectively. 2009 showed the same pattern, with the IT majors scoring an average of 83.7% on the cases and 79.0% on the test compared to the CJ majors, who averaged 31.9% and 68.9%, respectively.

The unfamiliarity exhibited by the CJ students with IT concepts and acronyms during the two semesters indicate that allowing them to take ITEC 5001U without completing all of the pre-requisites played a major role in their inability to succeed in the course.

Only one CJ student has enrolled in ITEC 5001U for the upcoming Fall 2010 semester. He has met all of the CS and IT prerequisites for the course.

3.4 ITEC 5002U

As stated previously, ITEC 5001U would be required for the IT major and that although required for the Cyber Security minor, ITEC 5002U would be an elective in the IT major. The combination of the need to teach required courses in the IT program of study and the loss of several IT professors has resulted in ITEC 5002U having never been taught since the minor was created. A list of lab software required for the course and a tentative syllabus were created, but the software was never purchased or downloaded, and the course was never implemented At the same time that the minor was initiated, control of the computer labs was transferred from the academic School of Computing to Computer and Information Services, further complicating the installation of any software needed for ITEC 5002U.

Since ITEC 5001U still contained some basic introductory material regarding more technical topics such as IDSs and firewalls, when ITEC 5002U was not scheduled for the 2008-2009 academic year, it was decided to keep such introductory material in ITEC 5001U.

ITEC 5002U has not been scheduled for the 2010-2011 academic year. Without the scheduling of ITEC 5002U, the minor in Cyber Security has become unattainable.

4. CONCLUSIONS AND LESSONS LEARNED

The creation of a Cyber Security minor at Armstrong Atlantic State University was a well-intentioned attempt at creating an interdisciplinary program in Cyber Security. As explained, two factors have led the faculty of the Department of Computer Science and Information Technology to revisit the viability of the minor. The first is that two sets of CJ students have not succeeded in what amounts to a more robust version of an introductory course in Information Security. The second is the inability to schedule the second Cyber Security course, ITEC 5002U.

There are several lessons that can be learned from this experience. The first is that prerequisites matter. They are created to determine a student's maturity and capability of learning a course's material. The desire to kick-start the minor should not have trumped the need to ensure that students were ready to succeed in the course. While the CJ students may have wanted to accelerate their completion of the minor, they would have been better off taking the time to complete the prerequisites.

It is possible that the obstacle of scheduling an additional 5000 level Cyber Security course could have been overcome by including another Criminal Justice course in the minor and either removing or purposely delaying the implementation of ITEC 5002U. Making it a required course for IT majors might have resolved this issue, as would have setting up different tracks within the IT major. However, given the current IT curriculum, it might be difficult to insert this as a required course into the four-year schedule.

Now that the labs used by CS and IT have been controlled by CIS for two years, the issue of installing security software in the labs has been eliminated. With proper requirement statements, it is possible to install and use such software in the computer labs used by the CS/IT department.

The return of ITEC 5001U to 3000-level status as ITEC 3100 has been discussed as a possible change. Such a change would certainly nullify the Cyber Security minor. However, any changes to ITEC 5001U and the minor's program of study will have to be approved by both Information, Computing, and Engineering and Criminal Justice and their respective colleges. There is a lot of curriculum committee work to be done before the minor is either removed or properly and fully supported.

5. REFERENCES

[1] AASU Undergraduate Catalog, AASU 2009-2010, page 257.

[2] AASU Undergraduate Catalog, AASU 2009-2010, page 184.

[3] Katz, Frank H., "Campus-wide Spyware and Virus Removal as Method of Teaching Information Security," presented at the *2006 Information Security Curriculum Development Conference (InfoSecCD 2006)*, September 22-23, 2006, Kennesaw State University, Kennesaw, GA.

[4] Wright, Marie and Kakalik, John, 2007, *Information Security, Contemporary Cases*, Boston, Jones and Bartlett Publishers, pp. v-vi.