ISSN: 2473-3857
v2 n4071

The Information Security Undergraduate Curriculum: Evolution of a Small Program

Lionel Mew
University of Richmond
lmew@richmond.edu
Richmond, VA

Abstract

In this paper, the author describes the curricular evolution of an undergraduate information security program at the continuing education school of a small liberal arts college. Significant changes have been made to the curriculum, with new courses, new structure and requirements and new technologies. The rationale and events behind these changes are discussed. Explanations of why these changes add value to the program provide readers with insight into factors causing the changes, and inform them on how similar changes may add value to their programs. The paper concludes with a list of rules of thumb used to select courses, make curricular changes, and espouse the programmatic philosophy of teaching to the real world and adding value to student portfolios as they enter the workforce.

Keywords: Security Curriculum, Curriculum Development, Cyber Security Education, Information Security

1. INTRODUCTION

This paper reports on how the curriculum for a new information security bachelor's degree program has evolved during the three years since its inception, as well as the motivation and rationale for the significant, albeit evolutionary, changes. In this case, the original degree program was designed to use as much of the existing information systems program as possible. Although that is not the best method of curriculum design, without following that process, the program would not exist today. Approval of the program, at a time of decreasing revenues, was predicated on limiting the initial investment. This requirement constrained the initial course offerings. This work discusses changes made to improve the program, and examines the justifications for each change.

The school of continuing studies at the author's small liberal arts college (SLAC) had a successful, traditional bachelor's degree program in information systems for well over 20 years. A post-bachelor's certificate in information systems (basically the major's portion of the bachelor's program) was also offered for career-switchers. In the 2012-2013 timeframe, enrollments dropped throughout the school, in all majors. Faculty and staff industriously looked for new ways to leverage competencies to devise new programs.

Information systems faculty were not exempt from the desire to create new programs. However, as information systems is a business competence, faculty were precluded from considering most of the typical avenues for expansion in the information systems area, such as offering a master's degree in technology innovation, due to potential conflicts with the institution's AACSB accredited business school. Consequently, it was decided to consider information security, as the business school had no security offerings or aspirations, and there were no security offerings from other schools within commuting distance. When researching the information security jobs market, a Burning Glass (2013) report found that information security job growth exceeded growth in overall computer jobs by 3.5 times, and exceeded growth in the general job market by 12 times. They found that this growth was widely spread across industries. The findings indicate that demand for information security professionals in the local metropolitan area rose from 1000 to 8,500 over the previous five years. With employers having difficulty filling information security positions, these jobs provide a salary premium of $12,000 over other computer jobs. Many of the high profile employers hiring information security professionals had a presence in the local area. There was a market and a niche for an information security bachelor's program.

The challenge was to develop an information security program using as much of the information systems curriculum as possible. Since most of the school's graduates stay in the local area following graduation, it was decided not to offer the type of program offered by institutions such as the University of Maryland. Those programs are oriented towards students seeking careers as government contractors or consultants, with courses oriented toward that end. For the same reason, it was decided not to follow a NSA CAE curriculum, nor to seek certification as such.

Upon reviewing the information systems major curriculum, it was thought that core courses of systems analysis, local area networks (LAN) and database design would be relevant to a student aspiring to a career in information security. Three existing elective courses, IT Security, IT Security Planning and Risk Management, and Introduction to Java, would also be relevant. One new course, IT Security Planning and Risk Management, would need to be added. By packaging these courses into a 21 credit hour major, a bachelor's degree in information security could be offered with only one new course. This new course was already extant, it had been offered as a special topics course for two semesters. Scheduling changes would be minimal, as current information systems majors would also be able to take the security courses as major electives. Since fewer than 25% of current courses would need to be changed or added to accommodate an information security major, accreditor notification, but not approval, would be required. The school started accepting students into the information security program in the fall of 2014.

Faculty and students had long desired an ethical hacking, or penetration testing course, before the new security major was even considered. Faculty believed that penetration testing was a relevant information systems competence, and offering a course in penetration testing would add to student repertoires as they enter the workforce. The problem was finding a qualified instructor. When an instructor was found, and a course developed for the fall 2015 semester, it was found that students majoring in information security had to take the course as a general education elective, since no provision was made for major electives. The fact that security students had to take a course which was a core competence for security practitioners caused program administrators to reconsider the program structure and ability to accommodate changes to field competencies with agility. A change to accommodate elective courses in the major was found to have a significant effect on the whole program structure, including required core courses. It was the first of numerous changes to keep the program relevant and add value to students.

2. LITERATURE REVIEW

There is still no standard curriculum for undergraduate programs in information systems security. Davis and Dark (2003) attempt to identify a core body of knowledge for a security curriculum, and to define a curriculum framework for programs in information assurance (IA). They consider curriculum design in terms of scope, order and sequence. Although the work is focused on IA programs for graduate computer science and engineering students, their plan to develop model curricula similar to the widely used and accepted Association for Computing Machinery (ACM) is of interest here. Indeed, although there is still no ACM guideline for information security, a report from an ACM working group (McGettrick, 2013) figured heavily in the design of the original curriculum. The focus areas and competencies noted in this report validated the proposed curriculum as sufficient.

Whitman and Mattord (2004) present a curriculum and courses for a security concentration within the existing technology curriculum models of Accreditation Board for Engineering and Technology (ABET) and ACM. They suggest that the lack of formal curriculum models leave institutions unprepared to offer the types of courses essential to the security professional. Shoemaker, Bawol, Drommi and Schymik (2004) present a delivery method for a curriculum based on the National Security Telecommunications and Information System Security Committee (NSTISSC) standard followed by institutions adhering to the National Security Agency (NSA) Curriculum. Bogolea and Wijekumar (2004) provide a case study examining security courses offered in a technology curriculum with the intent of synthesizing a security curriculum from the results. Petrova, Philpott, Kaskenpalo and Buchan (2004) discuss ways to integrate an information security specialization within traditional information technology programs.

Liles and Kamali (2006) present a curriculum designed for ABET accreditation, but aligned with NTISSI. Streff and Zhou (2005) present a case study of how their institution developed a security competence resulting in certification as a NSA Center of Academic Excellence.

Figg and Zhou (2007) present a curriculum for a digital forensics minor within an information security program. Mink and Freiling (2006) discuss their experiences offering offensive security tactics courses. Logan and Clarkson (2005) discuss issues involved with setting up a hacking lab.

In a paper on best practices for design and implementation, Mattord and Whitman suggest that, "a certain minimum degree of isolation is required for some InfoSec exercises and keeping the use of some software tools away from the campus network may be advisable (2004, p. 9)

3. Discussion

Major Electives

The first change to the program was caused by offering the aforementioned hacking course. Chagrinned that security majors had to take the course as a general education elective, administrators focused on providing opportunities for security students to take relevant elective courses within the major. It was noted that there are many experienced security practitioners in the local area who over the course of a career, have never participated in system development, have never worked with databases, and have never been developers or programmers. Consequently, it was decided to revise the required core courses to three: IT security, local area networking, and IT security planning and risk management. By removing systems analysis, database design and Java from the list of required courses, students could select the remainder of their 21 credit hour major courses from any number of security related courses offered.

New Courses

Following the change to accommodate major electives, administrators decided to add additional electives to keep the program relevant, and to give students additional competencies, particularly competencies arising due to emerging technologies and new paradigms from a practitioner's perspective.

New courses are generally added first in the form of special topics courses. These special topics may be taught twice, following which they may no longer be offered unless given a permanent course number and made a part of the curriculum. This offers the benefit of providing timely, relevant courses that meet the needs of industry. If the topic is a passing one, or not one desired to be a core competence, the course can be discarded after two offerings. If, on the other hand, a course is found to be a desired competence programmatically, or if it is popular with students, it can be made permanent.

The first new course offered was the aforementioned ethical hacking/penetration testing course. It was initially offered as a special topics course in offensive security tactics. The course was immensely popular with both security and information systems students, both because of a desire to develop this competence, as well as a general fascination with the topic.

The popularity of the course led to special topics courses planned to be offered next summer which enhance the penetration testing competence. These courses include malware reverse engineering, black hat python and the Metasploit Framework. Administrators prefer to offer core courses during the regular academic year, and special topics during the two 6 week summer sessions. These sessions allow students to dabble in topics they find of interest, without the depth required of a core course.

In addition to the hacking course, a desire to offer a digital forensics course predates the information security program, since it is an information systems competence as well. The reason it was not previously offered was the inability to find an instructor qualified to teach it. As this course comes to fruition, students are waiting for it with anticipation, and it will provide a useful professional competence.

Other new courses include geospatial information systems (GIS), Cloud computing, and IT security control and audit. For a small program, it is essential that elective courses offered are applicable to both information systems and information security majors. The Cloud computing and GIS courses were initially designed for information systems majors, so a significant security component had to be added to these courses to make them relevant to security students. This is not always possible. For example, it is unlikely that a forthcoming big data/NoSQL course will be approved for security majors.

Offering new courses in the form of special topics courses provides the program with the agility to capture emerging technologies and industry trends. However, the agility to offer such courses is dependent on the process by which such courses are approved. In this program, courses may be added at the sole discretion of the program chair. At a local community college, adding a new course requires the approval of a curriculum committee, as well as other steps such as demonstrating relevance to workforce needs, etc.

Course Sequencing

Many of the courses have obvious prerequisites, such as local area networking for ethical hacking and Cloud computing. However, in the information systems program, sequences were common. Courses such as introduction to programming could be followed by advanced programming, if a student was interested in making development a core competence. Likewise, a student interested in networking could follow the LAN course with an advanced networking course.

It was felt that similar sequences would add value to information security students by allowing them to specialize. Although the IT security planning and risk management course was an initial program offering, the addition of an IT security control and audit course could be touted as a sequence for students interested in becoming auditors or for those wanting to implement security controls. Similarly, students interested in developing a penetration testing competence could follow the ethical hacking and penetration testing course with follow-on courses such as malware reverse engineering, Black Hat Python, Metasploit, etc.

Course Delivery

It was found that technology and policy issues have a significant impact on the pedagogical delivery of course content. When the ethical hacking course was first offered, students used Kali Linux with VMWare installed in a standard computer lab. Upon review, the IT department forbade future use of VMWare for security labs. To solve this problem, administrators developed a plan to migrate all security labs to a cloud paradigm in the form of an Amazon Web Services (AWS) site. In the case of the hacking course, each student has an instance of Kali Linux to use on AWS, with target computers within AWS. This encapsulated paradigm mitigates the concerns of the IT department.

The migration to virtual labs in a cloud paradigm actually improves the pedagogical delivery of course content for most security courses. Having attack and target computers in an encapsulated environment allows students to practice using tactics and applications in a protected environment which may be unethical outside the cloud, if not completely illegal. The ability to develop competences using these tools gives students credibility when seeking employment as penetration testers or enterprise security architects. During an interview, they can explain to potential employers that they have actually used these tools.

Use of the Cloud also improves access and course administration. The extensibility of the Cloud allows instructors to simply add an instance of the lab environment if a student registers for the course at the last minute. If a hacking student destroys a target computer in the course of a lab, the instructor can immediately reset the computer with the touch of a click, or set the computers to automatically reset. Students are also able to easily access their lab environments from off campus or while traveling, without use of a Virtual Private Network (VPN) as was previously required.

In addition to hacking, numerous other security courses have the same constraints, and require similar environments. Examples include digital forensics, IT (LAN) security, the more advanced penetration testing courses, etc. These courses are all being migrated to the AWS environment. However, not all courses are being migrated. The university has an Oracle license that is supported on locally hosted servers by the IT department. The school is not charged for this, so there is no reason to change the status quo, and all database courses are anticipated to remain locally hosted until such time as something changes.

For most security courses, though, the use of virtual labs provides phenomenal benefits with few drawbacks. From a cost/benefit standpoint alone, there is no comparison.

Certificate Changes

When the information security bachelor's program was developed, a post-bachelor's undergraduate certificate of applied studies (CAS) in information security was also offered. The school had long offered a CAS in information systems. For this certificate, students had to complete the major's portion of a bachelor's degree.

When the security program was designed, the information security CAS consisted of only 12 credit hours. The intent was to provide a certification to legitimize prospective students already working in the security field. As 12 credits is an insufficient foundation for career-switchers, those wishing to transition were pointed towards the existing information systems CAS. In that program, students could take all of the security courses, if that was where their interest lay.

Since the program was initiated, transitioning students often enrolled in the 12 hour security CAS, since the lure of a short, inexpensive program outweighed the knowledge that the knowledge acquired was insufficient for the transition. CAS enrollment were also limited by the fact that as a 12 credit program, financial aid was not available.

When both local community colleges came out with 18 credit career studies certificates qualifying for financial aid, it was decided to change the CAS to match the length of the information systems CAS. To differentiate the program from the information systems CAS, the security CAS includes the same required courses that the bachelor's program requires as its core.

Assessment

Course assessment was originally problematic because of the certificate students. Bachelor's students had a fixed curriculum, and they were all required to take IT security planning and risk management, which required students to demonstrate all of the assessed competencies. However, certificate students were allowed to take any combination of security focus courses amounting to the requisite credit hours. Therefore, CAS students not taking the security planning course slipped through, resulting in the office of institutional effectiveness not being happy.

The problem was resolved with the change to the longer 21 credit hour certificate. The change to three required courses ensured that all CAS students will take the security planning course, and all will be participants in the assessments.

Training versus education

The discussion of training versus education is a long one and is beyond the scope of this paper. However, in their 2015 report, Burning Glass Technologies notes that 35% of Information security jobs require certifications, versus 23% of information technology jobs on the whole. The program does not want to get into the business of providing training and competing with commercial training providers. The hacking course is not designed to prepare students for the popular Certified Ethical Hacker or Offensive Security Certified Professional Certifications. It is designed to provide students with knowledge of the processes that professional penetration testers use. However, the fact that more than one in three security jobs have certifications in their descriptions cannot be ignored.

The courses, while not specifically designed as certification boot camps, arguably help students with the knowledge required for the certifications. One student in the IT security control and audit course recently successfully sat for the Certified Information Systems Auditor exam. The school is attempting to partner with some of the certification providers so students may receive discounts on certifications. Students seeking certification training are advised to take certification prep courses at local community colleges or non-credit courses offered by the university.

Standardization

When the original program was designed, it was decided not to seek certification as an NSA CAE. Most of the school's students stayed in the local area, where there are few opportunities for government work, whether as an employee, contractor or consultant. For that reason, the program was designed to provide students with broad competencies in enterprise security for medium sized enterprises.

Since the program was started, with the changes discussed in this paper being implemented, it was decided to work towards the CAE certification. New courses are being implemented to keep students relevant in the workforce. Many of the requirements for the CAE designation are already being done, such as sponsoring industry events and partnerships, sharing courses and faculty, community outreach, offering non-credit courses, etc., so the work would be mostly documentation.

The school typically serves as a degree completion program. Although it is possible to meet all of the requirements for a degree at the school, most students are admitted with 45-60 credit hours. Combined with such a small program, the school has to team with a community college to meet the CAE criteria. For example, the CAE criteria has a requirement for a lower level language. This program does not have the capacity to offer such a course. Therefore, students are pointed to the community college to meet that requirement.

One of the most compelling reasons to seek certification is one of standards. This paper has discussed the dearth of a comprehensive standard for information security education. However, as security matures as a sub-field, standardization is bound to happen. The CAE standard may not prove to be the widely accepted standard everyone uses, but it is a standard that we can work on now.

The ISACA Model Curriculum for Information and Security Management was also considered for possible alignment. Use of this model curriculum was initially felt as promising, as the program would not require significant changes to align with the model, and the one year experience waiver offered by ISACA would have been welcome. However, upon investigation, it was found that ISACA was not accepting alignment applications. Although the model curriculum is still a relevant to this program, without the legitimization of formal alignment, it was decided that the alignment effort would not be followed up at present.

4. SUMMARY

Numerous changes were made to the program in the two years of its existence. These include:

- Course electives were added to allow student choice in their programs. Electives have the advantage of allowing students to specialize and become professionally relevant.
- New courses were developed to maintain student interest and choice, and to give them relevant professional skills.
- Course sequencing helps students develop specializations and gives them a little depth in an otherwise broad program.
- Use of a cloud paradigm for labs improves the pedagogical delivery of course content.
- Changing the CAS from 12 to 21 credit hours enables a more thorough foundation and facilitates financial aid.
- Assessment is simplified when students are required to take assessed courses.
- Although higher education provides education rather than training, the fact that more than one in three security jobs required a certification must be considered.
- Although there are still no widely accepted standards for security education, standardization is a move toward goodness.

5. CONCLUSIONS

When developing this new program, factors other than the educational outcome had be accepted to establish the programs. A major constraint for program approval was to limit the initial investment. However, improvement must be a continuing process in the administration of any program. The best value is to keep the program relevant to student and workforce needs. Ways to accomplish this include integrating the ability to offer fresh courses and content, by offering students the sequences necessary to specialize, by leveraging technology, by offering the right programs for student needs and desires, by considering the need for certifications, by seeking standardization and most of all, to always focus on constant improvement.

6. REFERENCES

Bogolea, B., & Wijekumar, K. (2004, October). Information security curriculum creation: a case study. In *Proceedings of the 1st annual conference on Information security curriculum development* (pp. 59-65). ACM.

Burning Glass Technologies (2015). Job Market Intelligence: Cybersecurity Jobs 2015. [PowerPoint slides]. Retrieved from http://www.burning-glass.com/

Burning Glass Technologies (2012). Burning Glass Technologies: Initial Findings on Cyber Security Jobs. [PowerPoint slides]. Retrieved from http://www.burning-glass.com/

Davis, J., & Dark, M. (2003, June). Defining a curriculum framework in information assurance and security. In *2003 ASEE Annual Conference*, Nashville, TN.

Figg, W., & Zhou, Z. (2007). A computer forensics minor curriculum proposal. Journal of

Computing Sciences in Colleges, 22(4), 32-38.

Liles, S., & Kamali, R. (2006). An information assurance and security curriculum implementation. *Issues in Informing Science and Information Technolog*y, 3, 383-387.

Logan, P. Y., & Clarkson, A. (2005, February). Teaching students to hack: curriculum issues in information security. In *ACM SIGCSE Bulletin* (Vol. 37, No. 1, pp. 157-161). ACM.

Mattord, H. J., & Whitman, M. E. (2004, October). Planning, building and operating the information security and assurance laboratory. In *Proceedings of the 1st annual conference on Information security curriculum development* (pp. 8-14). ACM.

McGettrick, A. (2013). Toward Curricular Guidelines for Cybersecurity.

Mink, M., & Freiling, F. C. (2006, September). Is attack better than defense?: teaching information security the right way. In *Proceedings of the 3rd annual conference on Information security curriculum development* (pp. 44-48). ACM.

Petrova, K., Philpott, A., Kaskenpalo, P., & Buchan, J. (2004, October). Embedding information security curricula in existing programmes. In *Proceedings of the 1st annual conference on Information security curriculum development* (pp. 20-29). ACM.

Shoemaker, D., Bawol, J., Drommi, A., & Schymik, G. (2004). A delivery model for an Information Security curriculum. In *Proceedings of the Third Security Conference*.

Streff, K., & Zhou, Z. (2006). Developing and enhancing a computer and network security curriculum. *Journal of Computing Sciences in Colleges*, 21(3), 4-18.