An Undergraduate Information Security Program: More than a Curriculum

Belle Woodward
bellew@siu.edu

Thomas Imboden
timboden@siu.edu

Nancy L. Martin
nlmartin@siu.edu

School of Information Systems and Applied Technologies
College of Applied Sciences and Arts
Southern Illinois University
Carbondale, IL 62901-6614

ABSTRACT

This paper describes the implementation of an information security program at a large Midwestern university. The initial work is briefly summarized and improvements that have occurred over time are described. Current activities and future plans are discussed. This paper offers insight and lessons learned for organizations that have or are planning to implement an information security program. Some key success factors for this program have been a faculty project champion, faculty dedication and tenacity, involvement with industry partners, alumni, and students, and continuous improvement.

Keywords: Information assurance and security, Program assessment/design, Program improvement, Curriculum design and development, Advisory board

1. INTRODUCTION

Now more than ever, information security professionals are in demand in both government and private enterprise, and the trend is not expected to change any time soon (Frost & Sullivan, 2013, p. 565; Nakashima, 2013). As the education market exists today, the U.S. may not be in a position to quickly and adequately train the sizeable security workforce needed to secure critical infrastructure and key resources (Locasto et al., 2011). In order to meet this increasing need, more information security degree programs, especially at the undergraduate level, are needed to increase educational capacity. Currently, only a small number of academic programs are funded and equipped to formally train information security professionals and those few programs cannot train a workforce of thousands in a relatively short period of time (Locasto et al., 2011).

Given any number of constraints, however, it is possible for more institutions to rise to the occasion and develop security programs. This paper updates the endeavors of one university that has built a successful program over the course of several years. Relying upon the theoretical foundation of collaborative and active or hands-on learning, the authors of this paper had the opportunity to develop a new security curriculum beginning in 2006. Their work shifted the focus from one course in network security and two courses in networking that relied largely on abstract conceptualization and reflective observation to a more complete program fully equipped to train today's security professionals with an emphasis on hands-on experience (Woodward & Young, 2007).

A great deal of work has been accomplished besides the initial curriculum development. Through a comprehensive approach, and by working with industry partners, many other activities have been undertaken that have positively impacted the security program and the university. For example, hands-on labs were built; a Center for Information Assurance and Security Education was established; opportunities for student research, internships, and jobs were created; and ultimately the university received the federal government's designation as a National Center of Academic Excellence in Information Assurance Education (CAE/IAE) in 2010.

The following sections provide a brief summary of the building process and an examination of program success measures. Next, current activities and future plans that continue to grow the program are discussed. Finally, a summary of lessons learned is provided for others seeking to develop security programs.

2. BACKGROUND

In the early 2000's, many educators and institutions were implementing a variety of approaches to provide information security training (e.g. Surendran, Kim, & Harris, 2002; Whitman & Mattord, 2004). These approaches ranged from adding security content in other information technology (IT) related undergraduate and graduate courses or programs to full information security curricula.

During that time at the authors' large regional Midwestern university, a new course in security was added to the existing course lineup of two courses in networking to create the foundation of the security program. The courses were part of a degree program in information systems technologies and housed within a college of applied science.

Faculty further developed those three courses into an information security program consisting of 10 courses. Two development criteria for the new program were deemed most important: 1) use learning theory to guide program and course development which would ensure the inclusion of higher order and soft skill growth through hands-on, collaborative work, and 2) provide real-world experience by training students from a proactive as well as reactive viewpoint using real industry situations, scenarios, and exercises. Most of the details of the original program development are summarized in Woodward and Young (2007).

The curriculum was set up to mimic the multi-level technical support model (Walker, 2001) where basic skills are handled (or learned) at the first level, more advanced or complex issues are handled at the second level, and the most challenging or difficult problems are handled at the third level. The course names and numbers along with their relative level are listed in Table 1. For the purposes of this paper, the courses are labeled IS for information security.

Foundation Level
IS 121[1] - Installing and Upgrading Computers
IS 125[1,3] - Optimizing and Troubleshooting Operating Systems
IS 224[1,2] - LAN Installation and Administration
IS Level 1
IS 314[1,3] - Ethical and Legal Issues in IT
IS 316 - Information Assurance I
IS 335[2] - WAN Installation and Administration
IS Level 2
IS 360[2] - Network Security
IS 415 - Enterprise Network Management
IS Level 3
IS 392 - Special Security Projects
IS 416 - Advanced Enterprise Network Management

[1]Courses required of all department majors; [2]Original network and security courses; [3]Required course added after original program development

Table 1: Courses in the Program

In 2006, the new curriculum was formally mapped and submitted for evaluation to the National Information Assurance Education and Training Program (NIETP). In 2007, the university's courseware was certified as meeting all of the elements of the CNSS National Training Standards for Information Systems Security Professionals, NSTISSI No. 4011 and for System Administrators, CNSSI No. 4013. In 2012, the courseware was recertified through June 2017.

3. PROGRAM METRICS

The key to keeping any program or curriculum relevant is to continually monitor for needed improvements. Over the past six years, a number of indicators have been evaluated to make sure the program is headed in the right direction. Several are discussed below.

3.1 Enrollment

Of the 10 courses, six are electives. Enrollment in Level 1 and 2 courses is generally higher than in Level 3 courses because some students choose a few courses in the track as electives and do not complete all information security courses. Enrollment in the Level 3 courses is limited by equipment and faculty availability typically at a maximum of 18 students each semester. Figures 1, 2, and 3 reflect annual enrollments for each of the three levels of courses.

Level 1 courses have shown an upward trend although there was a drop in 2009. IS 316, the first Information Assurance course, has grown from 25 students annually to 84 students in 2011-2012. IS 335, the WAN course, has grown only slightly from 68 to the most recent count of 70 students. One factor that influenced the early enrollments for IS 335 was that students from an electronics technology major also took the course.

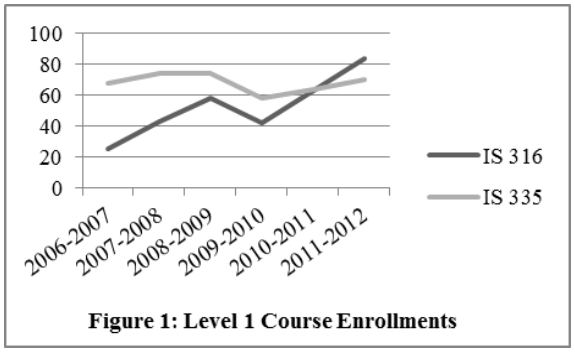

Figure 1: Level 1 Course Enrollments

Level 2 courses have also shown an upward trend. IS 360, Network Security, one of the original courses offered, grew from 44 students annually to 53 in the most recent count. IS 415, the first Enterprise Network Management course, has grown significantly from 9 students in 2006-2007 to 45 in 2011-2012.

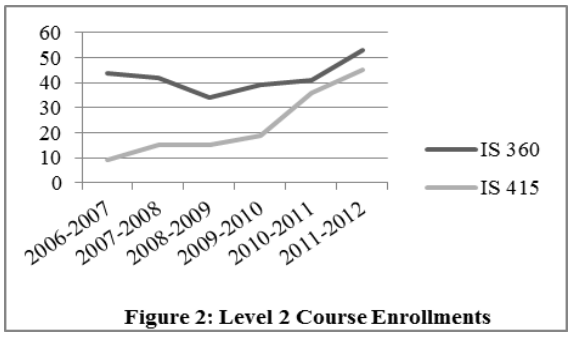

Figure 2: Level 2 Course Enrollments

Level 3 courses have also grown although Figure 3 appears to show an erratic trend recently. Both IS 392 and IS 416 scheduling was altered in 2012 to better accommodate a cohort of students. Hence, it appears enrollment has dropped when it was actually deferred into the next year. IS 392, Special Projects, is not required for the track and as such enrollment in this course is lower than the other courses. It was first offered in 2007-2008 with 15 students and saw a high enrollment of 20 students in 2010-2011. IS 416, Advanced Enterprise Network Management, began with annual enrollment of 17 students and in 2011-2012 had 34 students. Despite the uneven enrollments, the growth trend for both IS 392 and IS 416 are positive.

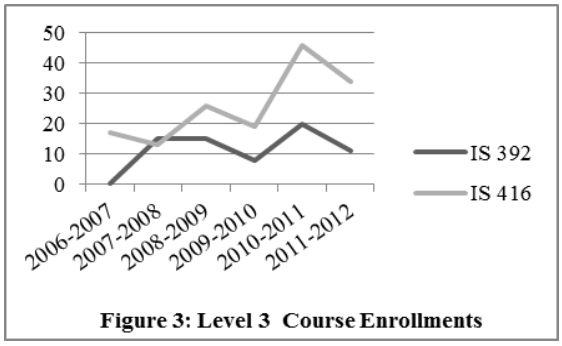

Figure 3: Level 3 Course Enrollments

Figure 4 displays enrollment in all six elective courses as a percentage of total students in the information systems technologies major. This particular measure is important since overall university enrollment has been declining because it helps explain the dips in individual course enrollment.

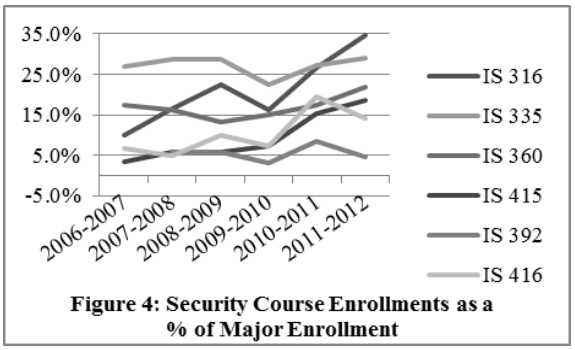

Figure 4: Security Course Enrollments as a % of Major Enrollment

Many factors may contribute to the growth in enrollment in this program. For example, the increased visibility of information security as a profession is likely the most influential factor. The enrollment increases are used as just one measure to aid faculty in program evaluation.

3.2 Job Placement

Placement rate may also be considered a measure of program success. Students are recruited from a variety of employers, from major international security companies to small locally owned businesses to government institutions of all levels. Many students have multiple job offers prior to graduation or a job offer immediately upon graduation, and approximately ninety percent are employed within six months after graduation. In a 2011 survey of graduates of the major, 28, or 39%, of respondents had completed the entire security track. Of that 28, 28% had an offer or were already employed prior to graduation. Only 3 graduates, or 11%, took longer than 9 months to find a permanent position. Figure 5 summarizes the time it took the graduates to obtain a job.

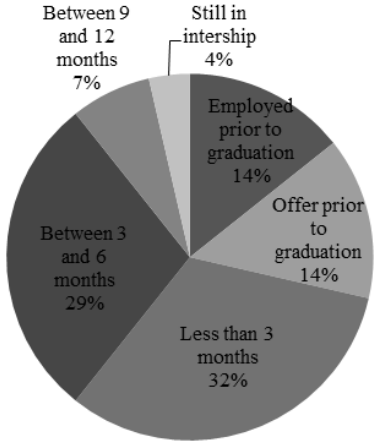

Figure 5: Time to Obtain a Job

3.3 National Center of Academic Excellence

Undoubtedly the most notable validation of the curriculum development efforts came when the program earned designation as a National Center of Academic Excellence in Information Assurance Education (CAE/IAE) from the National Security Agency (NSA) and the U.S. Department of Homeland Security (DHS) in 2010.

To qualify for consideration as a CAE/IAE, a number of requirements must be met. For example, information security had to be weaved throughout the departmental curriculum, not just in the information security courses. This effort involved the collaboration of all department faculty to integrate appropriate security topics into each course. Departmental faculty also had to show evidence of meaningful research in the area of information assurance. Evidence of student involvement in security activities and access to appropriate academic resources was also required. In the end, the work to earn the designation involved not only curriculum, but university wide support and involvement in matters related to information security.

4. OTHER PROGRAM ACTIVITIES

In addition to continually evaluating and enhancing the curriculum, many other activities are important to the growth and continued success of the program. Some of the most important activities are establishing and growing partnerships with industry, encouraging student involvement in extracurricular activities, and actively recruiting students into the information security curriculum and program. These activities often coexist or serve multiple purposes towards sustaining and growing the program, and four such activities are described below.

4.1 Center for Information Assurance and Security Education

In 2010, faculty began work to develop a recognized Center for Information Assurance and Security Education (CIASE) as a central focal point for student recruitment, student and practitioner involvement, interdisciplinary research projects, and other security related activities.

The CIASE's stated purpose is to promote information security education and practices not only among students and the university, but to the broader regional population as well. To accomplish that mission, the CIASE sponsors a variety of activities. The faculty frequently collaborates with various industry partners to enhance the curriculum and courses. These partnerships also provide internship opportunities for students and many times lead to grants and donations to the program from the partners. The CIASE also provides formal opportunities for undergraduate students to participate in projects and research with information security faculty.

The CIASE is home to two registered student organizations focused on security and technology. To meet the goal of broad regional impact, the CIASE has sponsored free workshops for the public on topics such as securing a home network. After much preparatory work and validation of efforts, the CIASE was formally recognized by the university in 2011.

4.2 Industry Partnerships

In order to provide truly rich hands-on experience, a considerable investment in lab equipment is required. Many institutions face economic barriers to providing new programs and survey results have shown that lack of funding and lack of equipment prevent some academic institutions from providing a hands-on learning component even in established security curricula (Martin & Woodward, 2012). Industry partners can be a valuable source of grant funding or direct equipment donations. Building and maintaining relationships with industry partners is at times a laborious task, but if the relationship is beneficial and not burdensome to the industry partner, it can be very fruitful for the academic program. While research about industry-academia relationships is minimal, some success factors have been identified including buy-in and support from company management and academia's commitment to contribute to industry needs (Wohlin et al., 2012).

This information security program began with networking hardware that consisted of hand-me-downs from the university's IT department as they replaced aging equipment with more modern versions. Over the course of time, it became clear that students were successfully retaining networking and security concepts and theory despite practicing on antiquated equipment. As the curriculum evolved and matured, hardware would break and be replaced by purchases from auction sites and stores selling refurbished equipment.

As students graduated and obtained employment at regional organizations, they began to "give back" to the program and solicit support from their employers. Representatives from the industry partners began attending university career fairs, sent alumni to classes to recruit students for internships and permanent positions, and perhaps most important, developed professional relationships with faculty. As this happened and as larger numbers of students applied to and obtained employment at partner organizations, it became easier for faculty and college leadership to ask for support in the form of equipment or other in-kind donations, contributions to scholarship funds, and even monetary grants for program improvement. For example, two large industry partners have provided more than $100,000 each in various forms of support over the past six years.

A benefit to the industry partners is that they often get the opportunity to get to know students outside the formal hiring process and to offer positions both temporary and permanent. Several partners reach out to the department in the middle of each fall semester and solicit student applicants for various opportunities. Summer interns at several partner employers more often than not receive offers for full time employment when they complete their studies.

Equally important to the success of the program as the equipment and funding donations received from industry partners is the advice, guidance, and support they provide for the curriculum. In October of each year, the program hosts a program advisory board meeting. Many of the industry partners mentioned participate in this event, which coincides with university wide career fairs, allowing them to make the most effective use of their time and travel. The advisory board members typically participate in a student-centric round table discussion, allowing students to solicit advice, ask technical or industry related questions, and introduce themselves to prospective employers. The advisory group provides actionable advice that is used to improve courses, programs, or the college as a whole. They discuss areas in which their recent intern and alumni hires are strong and other areas in which the faculty can concentrate on helping the students to grow.

An intangible but not to be overlooked advantage of having solid industry partners is the effect on recruiting. When speaking with prospective students, being able to tell the student that 15 graduates have gained employment at Company A or that 90% of the program's students who intern at Company B receive full time offers is testament to the ability of the program to prepare the student for a successful and rewarding career.

Currently, the university and the information security program have both formal and informal partnerships and relationships with various organizations. Several are multi-billion dollar companies with corporate headquarters within the state or region. Others are smaller businesses with a presence in the local community. Support can come from all

sizes and types of organizations. Regardless of the mix, without the strong support of industry partners, this program would not be nearly as successful as it has been. Through equipment and funding support, participation in advisory board activities, and by regularly employing student interns and graduates, the program's partnership with industry has been one of the most important keys to success.

4.3 Student Organizations

Another tool for helping to grow the program, recruit students, and perhaps most importantly provide students additional learning and growth opportunities are Registered Student Organizations (RSO). While several RSOs are active within the department, two are sponsored by security faculty and primarily participated in by students from the security program. One group is specifically security focused while the other focuses on broader IT areas through service learning activities at local non-profit organizations. While not formally documented, students find benefits in such projects similar to outcomes reported by others (Lee, 2012).

The primary focus of the security RSO is to provide a structured and formalized venue for students to study information security in preparation for participating in the Collegiate Cyber Defense Competition (CCDC). Students develop their own simulated competition environments in which they can observe, document, and respond to cyber attacks from their classmates as they learn offensive and defensive tactics. The group generally has about twenty active members; but only eight are able to compete in the cyber competitions. The group's official constitution provides a process for electing officers and competition team leaders as well as for selecting which students will compete. As an official RSO, the advisor provides minimal input to team selection but assists with training and helping to keep students motivated, and serves as the official team advisor for the competition.

In conjunction with the team's participation in this year's CCDC event, the RSO hosted "Cyber Security Day" for area high school and community college students. Attendees were able to observe the team while competing, hear speakers discussing information security topics, and participate in a mock cyber defense competition. Student volunteers helped run the event with the support of local businesses. The event helped to increase awareness of the program, provide a fun day of learning, and most importantly helped recruit future students.

The second RSO is not specifically focused on information security, but more on general IT topics and many security students also participate in this RSO. The group maintains two focuses: to provide students with learning opportunities outside normal classroom and to provide an avenue for local non-profit organizations to obtain technical support and assistance from students members.

This RSO routinely hosts speakers each semester and the sessions have been well attended. The speakers are usually solicited by the faculty advisor and are from local and regional technology businesses or even the campus IT department. The list below reflects a few examples of speakers who have provided talks to student attendees.

- An advisory board member spoke about the cyber security industry.
- A vice president for a local ISP discussed a large scale fiber optic project.
- A security analyst and researcher shared with the group what his job entails.
- A Special Agent from the FBI discussed a cyber crime investigation he was involved in.
- A detective explained cyber forensic investigations.
- The university data center manager gave a virtual tour of the campus facilities.

In general, invited speakers have felt very positive about their participation and most express interest in repeating the next year or speaking on a different topic sooner. At the end of each talk, most speakers make themselves available for informal discussion with students which may present an opportunity for employment.

The second focus of the RSO is on service learning by providing technical support and guidance to local non-profit organizations. Through word of mouth and minimal local press coverage, the group has received a host of requests ranging from security assessments to wireless network implementations to the creation of a custom database for tracking animals at a wildlife rehabilitation center.

Research has shown that these kinds of contacts among students and faculty outside the classroom are quite beneficial and "those which extend the intellectual content of the formal academic program into the student's nonclassroom life" are especially impactful ((Pascarella, 1980, p. 565). In the experience of this program, students involved in extracurricular activities with the faculty and other professionals, such as the RSOs, tend to be successful in their studies and during the job search, and many of these students continue to support the program as alumni.

4.4 Recruiting Activities

The faculty are regularly involved in outreach and recruiting activities and do not leave those efforts to the formal recruiting staff alone. Faculty and student representatives frequently participate in university and college level open houses and showcase events. Faculty participation in this part of the recruiting process is beneficial as it affords the prospective high school or community college transfer student the chance to meet those who will be their future instructors. The future students and their parents often have program or curriculum questions that may be best answered by an instructor and often times will continue to seek answers as they make final decisions on where to begin or continue their higher education.

5. FUTURE PLANS

This information security program is always evolving with new plans and activities. A few of those efforts are described below.

5.1 Distance Education

The department that houses the information security program was the first to offer a degree program entirely online at the university. The online students have traditionally followed a more generic curriculum since there were few information

security courses offered in an online format. However, over the last few years, the faculty has taken advantage of virtualization technologies to steadily increase the number of networking and security courses in the online program without sacrificing the hands-on aspect of the courses. By participating in academic partnership programs with VMware and Microsoft, the program is able to provide students with free academic licensing and software that has proven to be very useful for supporting online lab activities. VMware Workstation and VMware Fusion are two virtualization platforms students use to perform activities such as security software scans or launching attacks within an isolated virtualized lab environment.

In 2011, a university funding opportunity allowed for the purchase and implementation of a NETLAB+ system produced by Network Development Group. The NETLAB+ product relies on virtualization technologies as well as support hardware and infrastructure to allow students to have access to instructor created lab environments, including access to physical equipment such as routers and switches. Students use a web browser to connect to the NETLAB+ system and gain access to virtual machines and the available network hardware via the console ports. As NETLAB+ relies on VMware virtual machines, the same as used in many lab exercises in the traditional courses, it lends itself to very flexible and efficient migration of lab exercises to the online format. Online and traditional courses are gradually transitioning to the use of NETLAB+ for lab exercises as a variety of benefits are afforded by the system. These benefits include:

- Students can access the lab resources when most convenient for them.
- Faculty or lab assistants are not required to monitor student access to lab rooms and equipment.
- Faculty can quickly clone or delete virtualized lab environments as student demand fluctuates.
- Groups of several students can easily collaborate while working on lab activities.
- Original lab hardware and software states can be quickly reverted to in the event a student needs to redo a lab step or wishes to repeat the exercise.

In addition to the discussed instructor benefits of virtualization, students gaining familiarization with virtualization technologies provides yet another skill employers are more frequently seeking.

5.2 Core Curriculum Course

One way to better equip all students for their chosen career field is to expose as many of them as possible to information security principles. Inspired by others (Gandhi, Jones, & Mahoney, 2012), a freshman level core curriculum course in information security is currently in the planning stage. Although the particular course would not be required, it would be part of a menu of courses that all students must take to satisfy university core curriculum requirements. Not only does such a course inform students about the basics and importance of information security, it can serve as a recruiting tool as well.

5.3 Master's Degree Program

In an effort to keep pace with student interest and demand in graduate studies, a Master's degree program is under development. Students across the university and many area professionals have expressed interest in continuing their studies in an advanced information security program. Planning has been underway for some time to offer a post-baccalaureate program in information security with the goal of enrolling the first graduate students in the fall of 2015.

6. LESSONS LEARNED

Each institution will have a different path and different experiences when developing or growing an information security program. By documenting this program's efforts, hopefully insights emerge that will assist others seeking to fill the need for additional educational capacity in information security. Some of the key lessons learned from this multi-year endeavor are offered below. Lessons 1 and 2 date back to the original work to create the program that has been documented elsewhere (Woodward & Young, 2007).

1. Start with one person with a vision, a project champion. It may be difficult at times to sell the vision, particularly in difficult economic times, but commit to starting something with available resources. Project management literature is replete with evidence that an effective project champion is crucial to any project success and most agree that the champion is successful by voicing confidence in the project, including and motivating others to gain project support, and persevering under adversity (e.g., Howell & Shea, 2001).
2. Faculty dedication is key, especially if it means taking on extra load to make change happen. It will take buy-in from other affected faculty as well. If the long-term goal is to become a recognized CAE/IAE, it is especially important to gain that buy-in early on. Other faculty may already be covering security topics in their courses that can be built upon as the organization moves toward program recognition.
3. Equip labs by whatever means available. This program began with hand-me-down and, in some cases, obsolete equipment.
4. It takes much more than just a curriculum to build a successful program. As presented here, the curriculum is just the beginning. Get students interested and excited. Always strive to improve and expand the program's impacts.
5. Get industry support. It can come from large companies that perhaps already have ties to the university or small local firms that employ graduates. Industry partners need not be bound by geographic limitations especially when looking for potential financial support. Having industry relationships is critical for success in terms of donations, networking, educational opportunities, alumni opportunities, and even for recruiting when you can show prospective students where graduates find jobs.
6. Keep alumni interested and updated. Invite alumni to guest speak in classes or student organization meetings,

ask alumni to participate on an advisory board, and just keep in touch to kindle potential future collaborations. Often faculty learns of new technologies and tools through former students eager to share new things they have learned to help the program succeed.

7. Use social media. Yes, everybody is doing it, but keep it focused, meaning do not allow the information security specialty to become invisible inside of larger university groups. Create groups just for information security or just for the department. The connections between alumni, students, faculty, and industry partners can create unlimited synergistic opportunities.
8. Keep current. Perhaps it goes without saying, information security is highly dynamic, therefore the faculty must be passionate enough about the subject matter to keep up to date, literally on a daily basis. Being able to discuss a security incident or respond to something a student has read about reinforces their enthusiasm about the subject and in turn helps the program succeed.
9. As faculty, always evolve. Information security is not a subject like mathematics where the materials you rely on today will still be timely in five years, next year, or perhaps even next month. Therefore, the security courses need to keep pace. In this program, each semester faculty create new materials, assignments, course requirements, etc. that reflect events and updates in industry.
10. Take every opportunity to gain exposure for the program within the university, college, department, and community, and especially to prospective students. Looking back, this has been difficult at best because the program is "hidden" as a track inside another degree program. If this effort started today rather than seven years ago, the goal would be to create a separate degree in information security.

7. CONCLUSION

Demand for information security professionals continues to grow and more educational programs are needed to meet this demand. Although there is no one proven method for developing a program, hopefully this paper has provided other institutions with useful information needed to develop or to grow their own programs.

This paper has documented some of the work undertaken to create a successful information security program at a Midwestern university. The curriculum was developed based on learning theory and real world experience. Incremental improvements and extensions were made along the way and continue today. Industry partnerships were developed; equipment was gathered, primarily through grants and donations; students and alumni relationships were nurtured; and a host of other activities were undertaken.

It is evident from this journey that a curriculum is one end of a continuum that extends to full information security programs, CAE/IAEs, multiple levels of degrees, broader community impacts, and more. Each organization may choose to reside at different points on that continuum, but all can be valuable. Although each institution's endeavors are different, the goal of increasing educational capacity in information security is the same for all. The insights and advice provided can potentially assist others in building that capacity.

8. REFERENCES

Frost, & Sullivan. (2013). The 2013 $(ISC)^2$ Global Information Security Workforce Study. Retrieved June 12, 2013 from https://www.isc2.org/workforcestudy/Default.aspx

Gandhi, R., Jones, C., & Mahoney, W. (2012). A Freshman Level Course on Information Assurance: Can It Be Done? Here's How. ACM Inroads, 3(3), 50.

Howell, J. M., & Shea, C. M. (2001). Individual Differences, Environmental Scanning, Innovation Framing, and Champion Behavior: Key Predictors of Project Performance. Journal of Product Innovation Management, 18(1), 15-27.

Lee, R. L. (2012). Experience is a Good Teacher: Integrating Service and Learning in Information Systems Education. Journal of Information Systems Education, 23(2), 165-176.

Locasto, M. E., Ghosh, A. K., Jajodia, S., & Stavrou, A. (2011). The Ephemeral Legion: Producing an Expert Cyber-security Work Force from Thin Air. Communications of the ACM, 54(1), 129-131.

Martin, N., & Woodward, B. (2012). Building a Cybersecurity Workforce with Remote Labs. Information Systems Education Journal, 11(3), 57-62.

Nakashima, E. (2013, January 28). Pentagon to Boost Cybersecurity Force. *The Washington Post*. Retrieved February 12, 2013 from http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/19/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html?hpid=z1

Pascarella, E. T. (1980). Student-faculty Informal Contact and College Outcomes. Review of Educational Research, 50(4), 545-595.

Surendran, K., Kim, K., & Harris, A. (2002). Accomodating Information Security in our Curriculua. Journal of Information Systems Education, 13(3), 173-175.

Walker, G. (2001). IT Problem Management. Upper Saddle River, NJ: Prentice Hall.

Whitman, M. E. & Mattord, H. J. (2004). Developing and Teaching Information Security Curriculum. Proceedings of the 8th Annual Colloquium for Information Systems Security, West Point, NY.

Wohlin,C., Angelis, L., Phillips, L., Dittrich, Y., Gorschedk, T., Grahn, H., Henningsson, K., Kågström, S., Low, G., Rovegård, P., Tomaszewski, P., van Toorn, C., & Winter, J. (2012). Success Factors Powering Industry-Academia Collaboration in Software Research. IEEE Software, 29(2), 67-73.

Woodward, B., & Young, T. (2007). Redesigning an Information Security Curriculum Through Application of Traditional Pedagogy and Modern Business Trends. Information Systems Education Journal, 5(11), 3-11.

AUTHOR BIOGRAPHIES

Belle Woodward is a tenured, Associate Professor of Information Systems Technologies at the College of Applied Sciences and Arts in the School of Information Systems and Applied Technologies at Southern Illinois University Carbondale. She received her B. S. degree in Computer Science and Accounting (1989) at University of Bamberg in Germany and M.S. degree in Computer Information Systems (1997) from Webster University. Her research and scholarly writings have focused primarily on information systems pedagogy, e-learning/distance education, ethics, and information assurance. She co-authored several textbooks on networking and information assurance and has contributed over 25 refereed publications to the field. Her primary teaching activities have been in the areas of ethics, networking and information assurance. She has received numerous awards to excellence in teaching and research.

Thomas Imboden is an Assistant Professor in the School of Information Systems and Applied Technologies at Southern Illinois University. He studied networking and telecommunications and received a Bachelors and Master's degree from DePaul University in Chicago. Before teaching he worked as an information technology professional for ten years. He is currently pursuing a Ph.D. in Computer Science at SIU. He is the advisor for two technology focused student groups at SIU and teaches courses in networking and information assurance.

Nancy L. Martin is an Associate Professor in the College of Applied Sciences and Arts at Southern Illinois University Carbondale. She received her Ph.D. in Business Administration from Southern Illinois University and holds an undergraduate degree in computer science. She has 15 years of industry experience working with systems development and implementation. Her interests include IT ethics, IT curriculum and pedagogy, and healthcare IT. Dr. Martin's publications have appeared in Information Systems Management, Journal of Computer Information Systems, and Information Systems Education Journal.

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 1055-3096