Instructional Perspective on Cyber Defense: From Collegiate Competition to Capstone Course

Michael E. Whitman, Herbert J. Mattord
[1]Department of Information Systems / Coles College of Business
Kennesaw State University
1000 Chastain Road
Kennesaw, Georgia 30144
United States of America
{hmattord, mwhitman}@kennesaw.edu

ABSTRACT: *The creation of an experiential capstone experience for Information Security and Assurance students has been a decade-long challenge. Not long after security-based programs began offering degrees and concentrations in the discipline, the faculty struggled to create an industry-focused, balanced approach for security students. While some programs embraced the "capture-the-flag" approach to learning security through both offensive and defensive exercises, the faculty of the ISA degree program described in this article instead elected to adopt the purely defensive approach adapting a rapidly growing inter-collegiate competition structure as the capstone to their program. The purpose of this paper is share the experiences of the authors in planning and delivering that a cyber defense capstone course.*

Keywords: Cyber Defense, Capstone, Business Simulation

Received: 4 December 2013, Revised 14 January 2014, Accepted 18 January 2014

1. Introduction

In 2005, a group of researchers from the University of Texas, San Antonio (UTSA) made a presentation at the Colloquium for Information Systems Security Education (CISSE). During this presentation they introduced the concept of an inter-collegiate competition designed to allow information security (InfoSec) students to compete, head-to-head, in a defense-only style. Prior to this, most such competitions were in the style of "*capture-the-flag*", a combination of offense and defense with each team of students expected to defend an information system while simultaneously attempting to penetrate the defenses of the competition (White and Williams, 2005).

While entertaining for the students, the "*capture-the-flag*" style of contest (s.f. Sharma and Sefchek, 2007; Aman, Conway &Harr (2010); Booz Allen Hamilton, 2013; Chung, 2013; DEFCON, 2014;) was viewed by the UTSA researchers with some concern since the skills and abilities being promulgated did not align with those sought by industry and government in potential information security professionals. They noted that there were no competitions in place that emphasized the business service delivery model such as those found in competitions in other disciplines such as the National Collegiate Sales Competition (NCSC, 2014) and the like (White and Williams, 2005). The UTSA researchers proposed the development of a new competition, focused exclusively on defensive strategies, with real-world, business activities and tasks, where the student teams would be

expected to perform the tasks of an IT department in a small to medium-sized business (SMB) performing the tasks typical of IT employees including routine business tasks as well as specialized server and network administration functions (White and Williams, 2005). Now, after 10 years of competition, the National Collegiate Cyber Defense Competition (NCCDC) engages thousands of students from hundreds of institutions, across 10 regions (NCCDC, 2014a).

The authors of this paper were attendees at that first presentation, and became proponents of the concept of defense-focused student information security competition. The concept grew and became fully aligned with the objectives of the academic program at the author's institution. Over time, the undergraduate information security degree program at the host institution was updated to incorporate a capstone class that includes elements from the structure and design of the NCCDC. By expanding the delivery of the learning outcomes from the NCCDC model over the course of an entire semester it has become possible to leverage the concept of simulated business activities to engage students in an integrated experience that exposes them to the roles and responsibilities of InfoSec professionals. The purpose of this paper is to describe the NCCDC and its influence on the development, implementation, and evolution of the Cyber Defense course. The intent is to provide other institutions with insights they can incorporate into their own degree programs.

2. The Collegiate Cyber Defense Competition

Unlike traditional offensive and defensive security competitions, the NCCDC (www.nationalccdc.org) focuses on the simulation of practical InfoSec operations within a SMB. The entirety of the NCCDC competition is organized into three tiers: a state or regional qualifying competition, a regional competition, and the final national competition. The national final event is held annually in San Antonio, Texas (NCCDC, 2014a). Each of these tiers will be examined in turn, after a discussion of the format of the competition.

2.1 The NCCDC Format

The NCCDC – and by extension its regional qualification competitions – is designed to simulate a struggling SMB faced with an underperforming network and an insufficient security program. Each student team is assigned to a simulated regional business office that includes an identically configured portion of corporate system and network resources. Each of these regional office environments includes several functional servers and clients which are functioning to deliver simulated business services. The teams are expected to update, patch, re-configure, and harden these systems, while responding to ongoing requests for support from the business and also reacting to requests for business-mandated change. Meanwhile, a group of professional penetration analysts, designated as the red team, seeks to gain unauthorized access to team information and systems. Teams are scored based on their ability to: 1) maintain key services, 2) respond to business task assignments, and 3) protect against red team attacks.

2.1.1 The Systems and Services

Each NCCDC team is typically assigned to a business system environment that seeks to simulate those technologies and IT solutions in widespread use in industry. These include one or more network segments with multiples physical and/or virtual servers are providing essential business services. These services most often include static Web (HTTP), electronic commerce, email (SMTP), database, file services, domain service (DNS), and others. Each team begins with identically configured systems and networks. These must be used and maintained throughout the competition.

The services delivered by each team are continually assessed using a central scoring engine. This software determines whether the team is properly delivering all required services. The exact process of assessment varies from region to region. Some regions choose to award points for maintaining services, while others reduce point scores based on a percentage of availability to determine a score for the services category.

2.1.2 The Business Requests

Known in-game as injections, each of these tasks represent simulated business assignments. After assimilating the details of the request, each team will then plan and deliver the actions needed for each task's completion within the parameters provided. These actions may include addition, modification or deletion of users, software, services, hardware or networking components associated with the teams' resource base. It is estimated that the typical team endures a month's worth of work over the few days of the competition. The results of the teams' actions are assessed and successful and timely completion earns the team points.

2.1.3 The Red Team

Each NCCDC event involves the use of a pool of talented professional penetration analysts who volunteer as members of the red team. Several groups of volunteers from specific corporate and government agencies travel from region to region assisting each with their competition. The members of the red team assess each team's ability to resists attempts to compromise systems resources and steal simulated high-value information. The red team also performs various acts of malicious mischief often encountered in the business environment. In most events, successful red team actions result in penalty points assessed against the teams' scores. However, if the teams are able to perform successful incident response detection and reporting, the teams may mitigate some of the points lost.

2.2 Competition Stage 1: The State or Qualifying Competition

Each region of the NCCDC promotes either a state-by-state or central qualification competition. In the state-by-state model, an institution within each state associated with a region holds a scaled-down version of the NCCDC, to identify the top team per state to attend the regional. Alternatively, some regions host a physical or virtual qualification competition, where the top teams, regardless of state association, are invited to the regional competition.

Increasingly, regions are turning to institutions like Moraine Valley Community College, in Palos Hills, IL, home and the National Center for Systems Security and Information Assurance (CSSIA), to host a virtual qualification competition (CSSIA, 2014). Leveraging advanced technologies such as Network Development Group's NetLab+ (www.netdevgroup.com/products/), the CSSIA has become a national resource for regions without the technological infrastructure to host their own virtual qualification competition. Over a few weekend days, a region can engage dozens of competing teams in a qualifying event, and quickly identify the top teams to invite to an on-site regional.

2.3 Competition Stage 2: The Regional Competition

For the top teams from each state or virtual qualification competition, the next step is to travel to an on-site regional competition, held throughout the 10 regions in the NCCDC. The regions and the states they encompass are presented in Figure 1.

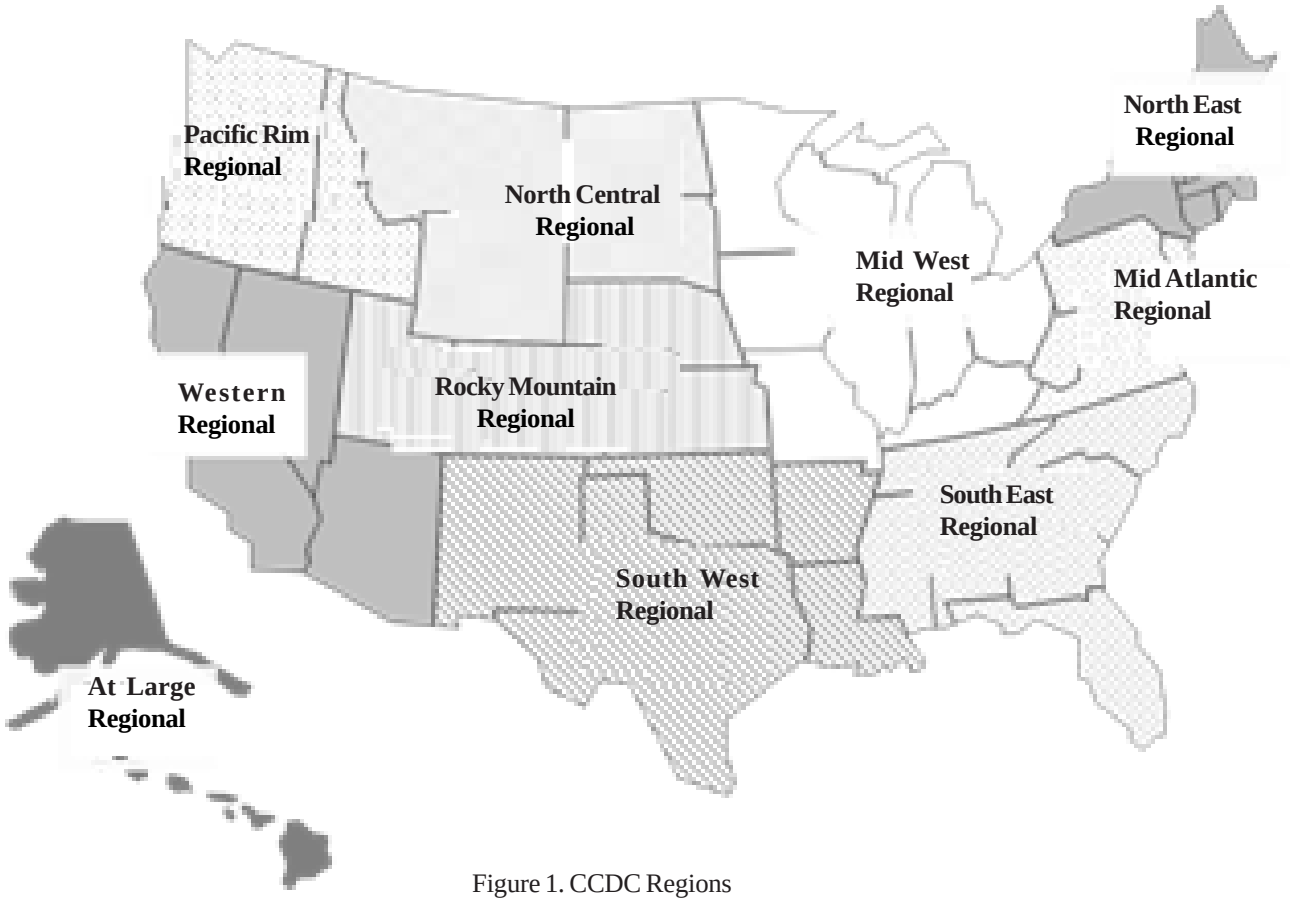

Figure 1. CCDC Regions

For those institutions that are unable to travel to a regional competition, an "*At-Large*" region was created, offering a purely virtual competition for those students in Alaska, Hawaii, and other locations too geographically dispersed to allow convenient travel (NCCDC, 2014).

While each region of the NCCDC is autonomous and offers its own variation of the competition, most incorporate 2-3 days of competition at a central location where teams compete. The winning team from each region advances to the national competition.

2.4 Competition Stage 3: The National CCDC

Hosted by UTSA, and conducted at the end of April annually, the national event is the culmination of the NCCDC season. Sponsored by the Department of Homeland Security and multiple industry partners, the National CCDC identifies the top team across the U. S. regions in a multi-day competition. For more information on the National CCDC, visit their website at www.nationalccdc.org.

3. From Competition To Capstone: The Cyber Defense Class

After successfully hosting a CCDC regional for several years, the authors became convinced that the critical skills and abilities learned and used by student competitors were the same as those sought by employers. They retain the opinion that those skills and abilities needed to be successful in the CCDC are a meaningful surrogate for those needed for success in the workplace. The experience of the competition offers students a valuable and important waypoint for InfoSec majors transitioning from academics to employment. As a result, the faculty members associated with the competition and with the then Bachelor of Science in Information Security and Assurance program began designing a course modeled on the core objectives of the NCCDC. The course, titled Cyber Defense was crafted to serve as an experiential capstone to the undergraduate degree program.

3.1 The BBA-ISA

Initially established as a Bachelor of Science, the undergraduate Information Security and Assurance degree (BS-ISA), at the time of its inception, was the first degree program of its kind at a public university in the Southeast, and only the second such program in the U. S. In its initial format, the BS-ISA incorporated a business and information systems course foundation, then required eight upper division ISA courses, and two major electives to complete, beyond the standard general education coursework. The list of initial ISA courses offered included:

- ISA 3100 Introduction to Information Security & Assurance (Required) – Prereq: Data Communications CSIS 2520
- ISA 3200 Applications in Information Security & Assurance (Required) – Prereq: ISA 3100
- ISA 3300 Policy and Administration Info. Sec. & Assurance (Required) – Prereq: ISA 3100
- ISA 3350 Computer Forensics (Elective) – Prereq: ISA 3100 & ISA 3200
- ISA 3396 Cooperative Study in ISA (Elective) – Prereq: ISA 3100
- ISA 3398 Internship in ISA (Elective) – Prereq: ISA 3100
- ISA 4210 Client Operating Systems Security (Required) – Prereq: ISA 3200
- ISA 4220 Server Operating Systems Security (Required) – Prereq: ISA 4210
- ISA 4330 Contingency Planning and Operations (Required) – Prereq: ISA 3300
- ISA 4400 Directed Studies in ISA (Elective) – Prereq: Varies
- ISA 4490 Special Topics in ISA (Elective) – Prereq: Varies
- ISA 4550 Security Script Programming (Required) – Prereq: ISA 4220
- ISA 4700 Emerging Issues in ISA (Elective) – Prereq: Varies
- ISA 4820 – Information Security & Assurance Programs and Strategies (Required) – Prereq: ISA 4330 & ISA 4220

In addition to the ISA courses, students were required to take two business classes, and three Information Systems (IS) courses.

In 2010, the faculty members of the Information Systems department decided to move the IS and ISA programs to the college of business, necessitating a conversion from a Bachelor of Science to a Bachelor of Business Administration structure. This resulted in the elimination of many of the upper division IS courses and the addition of a broader business core resulting in the BBA-ISA. The structure of the BBA-ISA program in general, and of the Cyber Defense course in particular reflect the core philosophy of the designing faculty: information security must consist of a careful balance of business and technical knowledge, skills and abilities. While some security-focused programs nation-wide are targeted more toward the technical side, this program seeks to produce a more balanced graduate that is capable of starting in variety of entry-level roles and is then capable of career progression up to the position of Chief Information Security Officer. As such, there is equal emphasis on technical expectations in the area (to include configuring and hardening systems and networks as well as exposure to technical control technologies such as firewalls and intrusion detection and prevention systems) and managerial expectations (such as policy development, risk assessment and risk management, security program management and implementation, strategic planning as well as governance).

The need to prepare students to exercise security management practices as well as demonstrate skills in network security have been priorities since information security entered the mainstream IS curriculum (Anderson and Schwager, 2002). Coupled with the full range of supporting topics such as access controls and applications security, the Cyber Defense approach to security capstones becomes the ideal mix of technical and non-technical topics.

Emphasizing the non-technical aspects poses a specific challenge as Beachboard and Beard (2005) state "…*students are simply more interested in writing programs and configuring systems than learning about administrative processes and thinking about fuzzy organizational issues. Given that most students do not expect to assume managerial positions immediately and that many of these same students feel that they do not receive a sufficient technical (read hands-on) education, establishing course relevancy poses a serious challenge*" (Beachboard & Beard, 2005). By integrating the technical and non-technical aspects of the competition into the course, the faculty felt they were able to mitigate this perspective and keep students focused on the end goals of operational, protected systems. A key component of the Cyber Defense approach is the emphasis on documentation and management of systems as well as the implementation of technical controls and security technologies (O'Leary, 2006; Whitman and Mattord, 2008).

The approach demonstrated in the Cyber Defense method breaks the traditional mold of lecture and test by minimizing actual content lectures, and emphasizing real-world scenarios, experiences and activities. Contemporary readings replace texts, and outside, industry speakers replace traditional instructor-led presentations, all focused on engaging the student, as has other programs (Beachboard and Beard, 2005).

3.2 ISA 4810: Cyber Defense

In 2005, shortly after returning from the CISSE conference in June, the ISA faculty quickly moved to create the new ISA 4810 Cyber Defense course. The course was submitted for approval in November 2005 and approved immediately. It was first offered the following Fall 2006. The initial intent was for the basic elements of a contest to remain, with the students working in teams to complete simulated business and technical assignments over a 16 week time frame rather than over a three day competition. The use of scenario-based courses is not novel or unique. In 2004, Grimaila proposed a scenario-based capstone experience for Texas A&M's graduate information security course, designed to integrate "*planning, analysis, design, implementation, and maintenance of an organization's information security program*" (Grimaila, 2004). While similar in scope to, yet predating the CCDC, this class incorporated both defensive and offensive security tactics, as students first built then rate systems, all in a business-based scenario that incorporated management decisions, budgets and risk management as well as technical hardening activities. In 2006, O'Leary similarly proposed a lab-based capstone course in computer security for undergraduates, much closer to the approach implemented as Cyber Defense. The Cyber Defense approach, rather than the capture-the-flag/attack-target is popular among IS-based information security programs, as it focuses on teaching "*potential security officers, rather than penetration tester*" (O'Leary, 2006). As Catougno and De Santis (2008) found:

"*In our game, instead of fighting against each other, student-teams had to cooperate in order to accomplish a list of businesslike tasks over a simulation of the Internet while preserving the security and availability of featured network services…The objectives of entities and people working on the Internet include sharing resources and data, providing and using applications and not just to set up networked systems running fictitious services, waiting for attacks. In the real world, Internet professionals set up services that have to work for a long time and be efficiently used as well as be carefully maintained. For these reasons*

we think that even though the cyber-war exercise paradigm gives an important educational contribution, it does not cover some relevant aspects of network security." (Catuogno and De Santis, 2008).

Naf and Basin (2008) discuss two approaches to developing security labs: a "*conflict-based*" approach-essentially the traditional capture-the-flag, offense and defense, version discussed earlier, and a "*review-based*" approach in which students build systems according to provided specifications, and then review each other's work, in more of an assessment approach like that found in certification and accreditation. The Cyber Defense approach is an extension of the review-based approach, where the review is performed in a "*conflict- style*" but not by the students, by experienced IT professionals recruited by the instructor specifically for this purpose. Students still build systems according to specifications, but must defend them against attackers. The critical distinction is the prevention of the sometimes mistakenly embedded belief that offensive capabilities are generally acceptable in the business world. While there is a time and place for penetration testing, this is conducted under strict agreements and control by an organization, and seldom by an inexperienced tester. Most organizations will not even employ a penetration tester, selecting to hire outside professionals, as it is possible to do more harm than good in the process.

The Cyber Defense course require prerequisites of both an operating systems security as well as a network security course. This is similar to other, established programs (Grimalia, 2004; Beachboard and Beard, 2005; O'Leary, 2006). The capstone course has gone through three phases of development so far, and is expected to continue to evolve as program needs mandate. This evolution has seen a waxing and waning of the use of the competition framework. The phases can be described as preparation, simulation, and modularization.

3.2.1 Phase 1: Preparation

In its initial offerings, the ISA 4810 course was treated as a senior-level seminar. In this format, each topic that could be isolated from the NCCDC body of knowledge was a seminar topic. Topics were many and varied and ranged from very technical to completely managerial. The list of seminar topics included roughly 25 items ranging from technical elements such as firewall configuration, domain name service architecture, system hardening, and malware detection to managerial topics such as project management, change control, policy management, and leadership skills. There were also blended topics that combined managerial and technical aspects such as intrusion detection and prevention system planning and deployment as well as security information and event management.

Each topic in the seminar mode included some degree of instruction, some element of research, and some form of peer communication. The instructional element was a lecture by the instructor or a guest speaker, an instructional Webinar and/or video presentation or supplemental reading. The research component was usually a research assignment leading the student to scholarly articles or professional-trade-reference books, but may include Web-based commercial sources for emergent topics. Peer communication included discussion boards, written papers subject to peer review as well as in-class presentations to share findings among the students.

After a period of time and when sufficient resources were present, the course was moved to its next phase, the use of simulation.

3.2.2 Phase 2: Simulation

In this phase of the course's delivery, the students were engaged in a group-based, semester-long, case-driven simulation. A case study that offered a suitably complex environment had been under developed by students in several consecutive Directed Study projects. This case set the stage for the multi-part simulation to improve the security status of the case's fictional organization.

The simulation aspect of the course was team-based. Students were assigned randomly to teams of 5 or 6 students. The number of students per team was intended to have sufficient capacity for relatively large and complex project work and still be small enough to maintain simplicity of organization and ease of communication. Team dynamics and performance issues proved to be a significant distraction to students and in some cases individual learning and assessed performance were negatively affected. While team working capabilities are and were a major learning objective for the ISA students, students offered energetic feedback that in early offerings, the course relied too heavily in team assessment of performance. In some cases, high achieving students felt that less motivated students did not fully support the team's objectives and may not have carried a fair share of the effort needed for team success. Each offering of the course was subjected to ongoing adjustments in assessment methods and relative weights to seek a balance between assessing the performance of the individual while still encouraging and assessing

team participation.

The basic approach of the course found each team assigned to a working, if poorly configured, computing environment. Each team simulated one geographic division of a larger organization. Using the case study as a backdrop, teams were required to go through a mandated security review and upgrade process. At midterm, each team performed peer-review penetration tests against an assigned team's updated environment. After communication of the results of the penetration tests, teams were required to remediate the systems and networks based on the reported results. The balance of the term was a sequence of injected changes. All of the simulation was performed against a backdrop of a simulated corporate culture with a project office, regular change control meetings and procedures as well as periodic malware and intrusion incidents. The final examination was a staged period of incident response with invited external penetration test staff assessing and compromising the student team's systems.

In retrospect, the simulation approach has been the most successful delivery model. This was in the face of concerns regarding team-based assessments and uneven performance/learning outcomes by individuals. Over time a robust peer assessment model was developed to allow supervised assessment of individual learning outcomes while assignments were performed in the team context.

The move of the ISA program from that of a Bachelor of Science to a Bachelor of Business Administration degree did not, on its own, materially change either the structure or content of this course. However a decision to offer the ISA program as a completely online program of study did. This decision was taken by the faculty shortly after the change to the BBA structure. The planned rollout necessitated that all required ISA courses be provisioned to the online delivery model mandated by the University. This requires that the capstone experience course needed to evolve once again to a model that would be better suited to that of an online course.

3.2.3 Phase 3: Modularization

The mandate for online delivery has seen a continued evolution of the capstone course and the deconstruction of the semester-long, group-based simulation. The longitudinal simulation was replaced with a sequence of topic-driven interrelated modules. In this format, the simulated business environment from the case study is retained. Rather than team-based project work, each topic found the students engaged in a structured sequence of activities taking them through the same fundamental steps that were present in the prior approach, utilizing the same extended case framework and the same expected learning outcomes. Group interaction was retained but the group assignments are not persistent over the semester, with the students reforming into new teams for each of the major project elements. The details of the team project specifications were carefully crafted to allow for remote group interaction to be sufficient to the needs of each project-based assignment.

Each of the course modules was given a common structure. First, the student was asked to review the learning objectives for the module and to understand to what level they are expected to perform. Then, a number of review materials were offered. These learning support materials included recap content from prior courses in the ISA course progression for those students who had not retained (or in some case acquired) key subject matter as well as some advanced content.

Using the modularized approach has allowed students to more effectively use virtualized and remote technologies to leverage the lab components of the course. Since each student was free to complete the modular elements without coordination of the technical infrastructure with other students, students may have chosen to work with University provided resources accessed with remote capabilities such as VPN connections supporting remote administrative access. Or, they may have chosen to virtualize the systems they used for the simulation and carried virtual operating systems with them on portable media.

3.3 The Pervasiveness of the Cyber Defense Course

In support of this paper, a study of existing Center of Academic Excellence in Information Assurance Education (CAE/IAE) programs sought to identify other institutions that were using courses similar to the Cyber Defense course previously described. The CAE/IAE program is a national recognition conducted jointly by the Department of Homeland Security and the National Security Agency. For more information on the program visit the NSA website at http://www.nsa.gov/ia/academic_outreach/nat_cae/. A list of CAE/IAEs was obtained from this website and each institution's web site was visited, identifying those programs with information security content, promoted as part of the CAE program. The course catalogs and description were scrutinized and a set of summary statistics collected about each program.

Over 150 CAE/IAE institutions were examined. Tables 1 and 2 provides basic demographic information regarding these security programs. In these tables, programs were first categorized as graduate or undergraduate and then identified as belonging in the disciplines of Computer Science (CS), Computer Science Engineering (CSE), Information Technology (IT), Information Systems (IS), Information Security and Assurance (ISA) (used to denote all security-focused programs) as well as a few programs that were truly hybrid (IS/IT and CS/IS).

Information Security-related Programs by Discipline/Major and Academic Level		
Discipline/Major	**Undergraduate**	**Graduate**
Computer Science (CS)	58	36
Computer Science Engineering (CSE)	6	3
Information Technology (IT)	22	8
Information Systems (IS)	20	10
Information Security and Assurance (ISA)	15	4
Hybrid - IS/IT	5	0
Hybrid - CS/IS	15	5
Totals:	**144**	**66**

Table 10. Identification of Security-related Programs in CAE/IAE Institutions

Information Security-related Courses by Discipline/Major and Academic Level		
Discipline/Major	**Undergraduate**	**Graduate**
Computer Science (CS)	168	120
Computer Science Engineering (CSE)	15	13
Information Technology (IT)	79	42
Information Systems (IS)	61	41
Information Security and Assurance (ISA)	192	36
Hybrid - IS/IT	5	0
Hybrid - CS/IS	15	5
Totals:	**535**	**257**

Table 2. Identification of Security-related Courses in CAE/IAE institutions

Cyber Defense-related Courses by Discipline/Major and Academic Level		
Discipline/Major	**Undergraduate**	**Graduate**
Computer Science (CS)	6 + (5)	0 + (4)
Computer Science Engineering (CSE)	1 + (0)	0 + (1)
Information Technology (IT)	2 + (5)	0 + (0)
Information Systems (IS)	0 + (1)	0 + (0)
Information Security and Assurance (ISA)	4 + (9)	0 + (0)
Totals:	**13 + (20)**	**0 + (5)**
Numbers indicate those courses which were clearly similar in nature to the Cyber Defense course described in this article. Numbers in parentheses may be Cyber Defense courses, but researchers were unable to positively determine based on the available information.		

Table 2. Identification of Security-related Courses in CAE/IAE institutions

Table 1 identifies the major type of the host programs for security-related concentrations and degrees. Some institutions had multiple degrees, both at the undergraduate and graduate level. By far the dominant model is a CS bachelor's degree with a security concentration. With only 15 institutions with a pure Information Security Baccalaureate degree, and only 4 with a graduate degree. All others reviewed were concentrations in existing degree programs.

Surprisingly, as shown in Table 2, there are over 535 courses in undergraduate degree programs versus 257 in graduate programs. In its early stages the CAE program attracted more graduate than undergraduate programs, as the NSA sought to attract future researchers in security-related fields like cryptography. There are also more courses in ISA programs than in CS programs, the leading security-concentration discipline.

Table 3 shows the number of confirmed Cyber Defense courses at other institutions. Thirteen other institutions had courses that were very similar to the Cyber Defense course described here, whether they were labeled as such or not. In some institutions, the course was called "*Advanced Network Security*", while in a few others it was labeled "*Applied Security Lab*". In at least four institutions, it was explicitly labeled Cyber Defense. With potentially double that number considering the potential Cyber Defense courses, it appears the authors were not the only faculty who felt this approach has merit. As graduate programs are almost explicitly research degrees, it was not surprising to find that very few with technical hands-on security courses, and most focused on a research oriented methodology.

3.4 The Future of the Cyber Defense Course

As the SECCDC continues to progress, and the demands of future employers are refined, the ISA 4810 Cyber Defense course similarly continues to evolve. Since its initial inception, the course has and will continue to be modified regularly, as part of institutional Assurance of Learning efforts.

4. Next Steps in Cyber Defense Courses

We believe that the future of Cyber Defense course offerings lie in virtualization. With the incorporation of VMWare IT academy licensing into a program's infrastructure, students can be led to master not only server administration, but also virtualization technologies. At the current time many courses of this type incorporate a number of virtualization requirements. Virtualization technologies have long been recognized as a method of leveraging the limited resources available to faculty teaching laboratory courses (Lunsford, 2009), providing flexibility in the instruction of information security, while working with the systems constraints of the institution and its need to provide general laboratory support for multiple classes of student learning. Rather than converting an entire lab to OpenSUSE Linux for example, an instructor can deploy virtual machines (VMs) providing virtualized instances for students to work on, without changing the existing structure of the underlying lab infrastructure–beyond installing a VM client.

A possible next step for courses of this type are to move the course infrastructure from locally managed servers into a private cloud environment, based on the use of VMWare ESXi servers controlled by a Network Development Group NetLab appliance. The purpose of this appliance is to provide a single configurable environment incorporating various labs organized into "*pods*" where students and student teams can access and conduct various information security labs, ranging from instanced, single system exercise, to persistent, multi-system development exercises. It is the latter where the environment provides support to the Cyber Defense Course. Rather than requiring the students to physically access a computer lab, or use VPN technologies to remotely manage their cyber defense systems, this environment allows individual students to log into the appliance using a standard Java-enabled web browser, and manage all devices remotely. Such a system msyalso provides the following benefits:

- Preconfigured lab exercises to support Cisco, VMWare and other Cyber Security licensing.
- A scheduling function to control student access, and prevent overtaxing system resources.
- ESXi server integration and control – allowing the instructor to configure the infrastructure containing multiple ESXi servers as a single cloud-based environment.
- Simplified web-based administration for both the technical infrastructure and student access controls.

While not inexpensive to implement, such an environment has the potential to dramatically reduce the need for physical labs as students both on and off-campus may be able to access the virtual environment and conduct their labs. A capstone course can then be positioned to take advantage of a virtual NetLab architecture.

As the needs of the business community continue to evolve, and thus the structure and focus of anycapstone course like Cyber Defense will also change. While the specific elements of specific courses of this nature will vary, the overall learning objectives and instructional focus remain similar: to prepare students to work in modern information security operations, performing both business and technical tasks.

References

[1] Aman, J., Conway, J., Harr, C. (2010). A Capstone Exercise for a CyberSecurity Course *Journal of Computing Sciences in Colleges*, May, p. 207-212.

[2] Anderson, J., Schwager, P. (2002). Security in the Information Systems Curriculum: Identification & Status of Relevant Issues, *Journal of Computer Information Systems*, Spring, p. 16-24.

[3] Beachboard, J., Beard, D. (2005). Innovation In Information Systems Education-Ii Enterprise Is Management: A Capstone Course For Undergraduate IS Majors, *Communications of the AIS*, 15, p. 315-330.

[4] Booz Allen Hamilton (2013). KAIZEN, A CTF Presented by Booz Allen Hamilton, Black Hat 2013. WWW Document viewed 5/28/2014 from http://www.blackhat.com/us-13/sponsored-workshops.html#Booz.

[5] Catuogno, L., De Santis, A. (2008). An Internet Role-game for the Laboratory of a Network Security Course, The 2008 Annual Conference on Innovation and Technology in Computer Science Education (ITiCSE'08), Madrid, Spain, p. 240-244

[6] Chung, K. (2013). CSAW CTF 2013, WWW Document viewed 5/28/2014 from https://ctf.isis.poly.edu/about/.

CSSIA. (2014). National Center for Systems Security and Information Assurance: Innovation in Cyber Security Education. WWW Document viewed 5/28/2014 from http://www.cssia.org/.

[7] DEFCON. (2014) DEFCON CTF History. WWW Document viewed 5/28/2014 from https://www.defcon.org/html/links/dc-ctf-history.html.

[8]Grimaila, M. (2004). A Novel Scenario-Based Information Security Management Exercise, *In*: Proceedings of the 2004 Information Security Curriculum Development Conference, Kennesaw GA. p. 66-70.

[9] Lunsford, D. Virtualization Technologies in Information Systems Education, *Journal of Information Systems Education*, 20 (3) 339-348.

[10] Naf, M., Basin, D. (2008). Two Approaches to an Information Security Laboratory, *Communications of the ACM*, December, 51 (12) 128-142.

[11] NCCDC. (2014a) The National Collegiate Cyber Defense Competition. WWW Document viewed 5/28/2014 from http://www.nationalccdc.org/.

[12] NCCDC. (2014b) National Collegiate Cyber Defense Competition. WWW Document viewed 5/28/2014 from http://www.nationalccdc.org/index.php/competition/about-ccdc/history.

[13] NCSC. (2014). National Collegiate Sales Competition.WWW Document viewed 5/28/2014 from http://www.ncsc-ksu.org/

[14] O'Leary, M. (2006). A Laboratory Based Capstone Course in Computer Security for Undergraduates, ACM Special Interest Group on Computer Science Education Conference (ACM SIGCSE'06). p. 2-6.

[15] Sharma, S., Sefchek, J. (2007). Teaching information systems security courses: A hands-on approach, *Computers & Security*, 26, p. 290-299.

[16] White, G., Williams, D. (2005). The Collegiate Cyber Defense Competition, *In*: Proceedings of the 9th Annual Colloquium for Information Systems Security Education (CISSE), Georgia Institute of Technology. Atlanta GA. P. 26-31.

[17] Whitman, M., Mattord, H. (2008). The Southeast Collegiate Cyber Defense Competition, Kennesaw, GA: Proceedings of the 2008 Information Security Curriculum Development Conference. Kennesaw GA. P. 1-4.

Author Biographies

Michael E. Whitman, Ph.D., CISM, CISSP is a Professor of Information Security and Assurance, Department of Information Systems, MichaelJ. Coles College of Business, Kennesaw State University, Georgia, where he is also the Director of the KSU

Center for Information Security Education. He currently teaches graduate and undergraduate courses in Information Security and researches in areas of information securitypolicy, administration and governance, and computer use ethics. Dr. Whitman has several textbooks in print and has published articles in Information Systems Research, the Communications of the ACM, the Journal of International Business Studies, Information and Management, and the Journalof Computer Information Systems.

Herbert J. Mattord, Ph.D., CISM, CISSP is an Associate Professor of Information Security and Assurance at Kennesaw State University, Kennesaw,GA. He completed 24 years of IT industry experience before joining the faculty at Kennesaw State University in 2002. He was the Manager of Corporate Information Technology Security at Georgia-Pacific Corporation,where much of his practical knowledge was acquired. He currently teaches undergraduate courses in Information Security and also researches in the are as of web-based authentication and information security management. Dr. Mattord has several text books in print and has presented at the AmericasConferenceon Information Systems and published in Information Resources Management Journal.