

Developing and Implementing an Institution-Wide Introductory Cyber-Security Course in Record Time

Christopher Brown, Frederick Crabbe, Rita Doerr, Raymond Greenlaw,
Chris Hoffmeister, Justin Monroe, Donald Needham, Andrew Phillips,
Stephen Schall, John Schultz, Steven Simon, David Stahl, Sarah Standard¹

United States Naval Academy
Annapolis, Maryland 21402

ABSTRACT

In spring 2011, the United States Naval Academy decided that, beginning in fall 2011, all first-year students would be required to take an introductory core course in the technical foundations of cyber security. This decision triggered our attempt to set an “academic world-record” for the development and implementation of a unique core course in six months time for all 1,200 incoming Midshipmen. The concern was that many graduates lacked an understanding of the risks and threats pertaining to cyber security, as cyber attacks and cyber crime become greater threats to the health and preservation of the nation. Such instruction simply could not wait; it had to be done, and done immediately. Throughout this paper we present the lessons we learned to provide guidance to others faced with the similar challenge of implementing a university-wide course while under a tight deadline. The insights we gained will prove useful to those thinking of implementing a technical core course, particularly one in cyber security.

Categories and Subject Descriptors

K.3.2 [Computers and Education]: Computer and Information Science Education – *curriculum, information systems education, literacy*; K.6.3 [Management of Computing and Information Systems]: Installation Management – *computer selection, pricing and resource allocation*; K.6.3 [Management of Computing and Information Systems]: Software Management – *software selection*

General Terms

Design, Documentation, Security

Keywords

Cyberspace Policy Review, Cyber-Security Education, Hands-On Laboratory Exercises, Information Assurance, Logistics, Naval Academy

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

ACMSE'12, March 29–31, 2012, Tuscaloosa, AL, USA.
Copyright 2012 ACM 978-1-4503-1203-5/12/03...\$10.00.

1. INTRODUCTION

The United States Naval Academy (USNA) is charged with ensuring that all Midshipmen (undergraduate students at USNA) receive an education that is sufficient to prepare them to preserve, protect, and defend the nation. Influenced by President Obama’s May 2009 Cyberspace Policy Review, which included the need to “expand and train the workforce, including ... cyber security expertise in the Federal government” [7], a committee of USNA faculty members were charged with exploring and defining the scope of understanding of cyber security needed by Midshipmen in their capacity as future naval officers. The committee worked with the Office of the Chief of Naval Operations and Commandant of the Marine Corps staffs, analyzed the other service academies’ inclusion of cyber-warfare concepts in their curricula, and examined various other academic cyber programs. Note that for the purposes of this paper, we use the term “cyber” to refer to the totality of the space in which new kinds of computer crime, terrorism, espionage, and warfare are taking place.

In August 2009, USNA’s Cyber Warfare Ad Hoc Committee delivered its Initial Report that included a recommendation to create a required core course providing a technical foundation for undergraduate cyber-warfare education for all students regardless of academic major [6]. The unanimous view of the committee was that the course be technically oriented, focused on naval applications and case studies, and delivered in a hands-on, lab-based format. This course was intended to form the technical basis for continued cyber-security education that could be expanded upon as appropriate within the various majors.

In April 2010, USNA’s Academic Dean & Provost formed a second committee, the Ad Hoc Committee on Cyber-Security Curriculum Options, charged with examining a variety of approaches for integrating cyber concepts in the core curriculum, and ultimately they recommended a two-course, technically-oriented sequence: the first to be taken by all students during their initial year and the second, providing more technical depth, to be taken by all students during their third year. This paper focuses on the development and implementation of the first in that sequence of two cyber core courses.

Although USNA settled on one course in the first year and a second course in the third year, numerous other options were considered. None of which were deemed easy to implement. At the time the options were formally presented (February 2011), the general consensus of the Committee and all others who had been involved was that the earliest possible implementation date for

¹ Contact author phone and email: 410-293-6756, standard@usna.edu.

any option selected would be August 2012. In February 2011 the Committee's recommendations were approved, but the implementation date was to be August 2011—a mere six months later. There were many “roadblocks” to overcome to meet this deadline, some that would be typical of any academic campus (such as faculty-led, curriculum-review processes and faculty-senate votes and recommendations). In this instance, the ground rules usually applied at USNA were modified given the short deadline and also the importance of the initiative being undertaken. USNA leadership made two things clear from the outset: the implementation deadline of August 2011 was immovable, and the inclusion of the new cyber course as a first-year, lab-oriented, technical-core course was non-negotiable. Other than that, all other specific details from course content to faculty development to assessment measures were left up to the faculty to debate and decide. So, in that context and with only six months to act, all faculty approval processes were conducted *in parallel* with the actual course development and implementation planning.

There were many other significant challenges as well, ranging from determining what technical content to teach, to who would teach the course and how USNA would identify and educate those faculty members, to acquiring necessary hardware and software. This paper describes these obstacles and explains how they were overcome within a very limited, six-month time frame.

2. CYBER SECURITY PROTOTYPE

Although USNA had been teaching two information-assurance courses for several years, these courses could only be taken by Computer Science (CS) and Information Technology (IT) majors, limiting the exposure of the material to a narrow slice of the student body. The Final Report of the Dean's Cyber Warfare Ad Hoc Committee in August 2009 recommended that USNA “create a required computer science technical core course that addresses the technical foundations of Cyber Warfare” [6]. This recommendation became the fundamental content statement for the course: that it should focus on the technical foundations of cyber security, enabling other courses to include related content on policy, psychological operations, and similar issues later in the curriculum. At the time, no prototype course existed.

2.1 Development and Testing

Based on the prospect of a required course for all first-year students, USNA offered a pilot course in the spring of 2010. It was run as a four-credit, five-hour per week course for non-CS/IT majors, with three lecture hours and a two-hour lab. The prototype included eleven weeks of basic computing material (problem solving, basic programming, web pages and JavaScript, databases and spreadsheets, hardware, and networking), followed by five weeks of cyber security content. The justification at the time for the heavy concentration on CS material at the beginning of the course was an assumption that the students would be unable to understand the technical cyber-security material without a broad understanding of the major hardware and software systems in a computer.

In fall 2010, the USNA Dean requested a version of the pilot course in a format requiring only three credits and four total hours of class time (which included a two-hour lab period) that could be taught to all first-year students. We began with the content taught the previous spring, then redistributed much of the background knowledge so that it was introduced together with the computer

security concept to which it applied. For example, JavaScript would be introduced in the context of server attacks. We dedicated more of the available lecture and lab time to hands-on activities, both to follow the guidance provided by USNA's Cyber Warfare Ad Hoc Committee and to incorporate the recommendations of students who had experienced the original prototype. We also reduced the number of lecture hours dedicated to teaching programming. The resulting proposal had four modules: three weeks on the basics of hardware and software, three weeks on web-based attacks, three weeks on the basics of networking, and about seven weeks on cryptography, forensics, attack, and defense. The new course content was positively endorsed by numerous Navy cyber commands and ultimately became the basis for a second prototype offered in the spring of 2011 and the course that was submitted for approval to the USNA curriculum committee. Following approval, course content continued to evolve. All modifications were based on student feedback and lessons learned through the delivery of the second prototype. The composition of the curriculum, as delivered in the fall of 2011 is described in section 3.

2.2 Lessons Learned

In the end, the most important lesson from the first pilot course was that the students did *not* need to be able to write their own programs, but rather that they only need to be able to understand and modify elementary existing programs or code fragments. When we ran the second pilot course with the new model, we found that students were able to concentrate more on the effect of a code fragment rather than on how to write the fragment. In other words, students were able to focus on the security implications of the code, rather than its syntax. The second pilot course also revealed the need for a canonical network service that could be simplified and generalized to emphasize the principles of cyber security as well as more experiential learning.

3. BRIEF CURRICULUM OVERVIEW

3.1 Content and Considerations

The current course consists of three major content sections: the Cyber Battlefield, Models and Tools, and Cyber Operations. In the first section, the Cyber Battlefield, students learn about digital data, elementary concepts in computer architecture, operating systems, programs, the web, networks, wireless networks (including WEP cracking and wireless sniffing), and the Internet.

In the second section, Models and Tools, students learn the basics about formal models of security and risk in information systems. With this newfound knowledge of what computer security means, they then are exposed to some basic tools for providing security: firewalls, symmetric encryption, cryptographic hashing, asymmetric encryption, and digital certificates. In the final section, Cyber Operations, students learn about cyber recon, attack, defense and forensics, and they review case studies.

The topic list just presented can be daunting, especially in view of the target audience—first-year students with no prior experience—and the commitment to being academic, technical, and hands-on. Here are a few of the considerations that went into covering this material in a meaningful way:

- We used the web (for example, web-servers, browsers, HTTP, and so on) as the focal point for our course content, using that as an example from which additional concepts (and applications) could be explained and understood. In this way, the students would focus in detail on something simple

and familiar (the web), and from which they could grasp specific concepts via hands-on experiences, and then use those examples and experiences to understand other topics by analogy, generalization, or contrast. Not only is the web an important domain for cyber security, but it was our canonical example for understanding network services. Other network services could be meaningfully understood by their similarities to and differences from the web.

- We looked for opportunities to repeat the same concept in multiple places and to refer back to earlier encounters with it explicitly. For example, the difficulty of dealing gracefully with unexpected input was covered in the lessons on programs, in the HTML/JavaScript injection-attack example, in attacks on network services, and yet again in discussing the vulnerabilities exploited to install malware.
- We carefully scrutinized what to cover and in what depth to cover it. Our goal was to provide simplified models of key technologies from which students could reason correctly—up until the point that the simplifying assumptions were violated. For example, one good choice for simplified content was to present the web simply as clients making GET requests to servers. We left out details like proxies, POST, and many more, but we were able to do a lot with the simple model. Such simplifications did not always work though—for example, pretending that a router has one IP address rather than one for each interface. Once we reached the network recon section, students were seeing traceroute data that they could not reconcile with the simplified model.

Course material—student lecture notes, lab instructions, homework assignments, and miscellaneous resources—were all available to students via a course webpage. This material is comprised of over 36,000 lines of locally developed HTML, as well as numerous PDF files, image files, and programs. Since the course was not available elsewhere in a textbook format, the lesson material, homework, and labs were all developed by the course coordinator and development team. A custom textbook consisting of selected chapters from four other textbooks was developed for the course. The students were required to purchase the textbook, but it was not utilized as a primary source for instruction.

3.2 Lessons Learned

The key lessons learned in the development of the curriculum were to be highly selective in the foundational content to cover; to find ways to integrate material multiple times, to simplify explanations of new material, and to provide a framework for analogy, generalization, and contrasting items; to exclude any expectation of learning to write programs (after all, this is not a programming course) and yet still be able to understand the logic in elementary programs themselves; and to choose carefully which topics to pursue in depth. Hands-on activities were devised and incorporated into the lectures. The activities were designed to enhance student understanding and we found that the time spent conceiving the activities was worthwhile since the students' responses on course surveys indicated that the activities were extremely helpful. We learned that it was unreasonable to expect total agreement by the faculty developers (and instructors) on all

aspects of the curriculum. The key was to allow multiple forums for the discussion of issues, and we used weekly meetings, reports, and instructor-email lists to accomplish this information exchange.

4. LOGISTICS

4.1 Hardware Setup

All students at USNA are required to purchase a computer whose requirements and configuration is determined by the USNA Information Technology Division. Beginning with the class of 2015, the first-year Midshipmen all have laptops to use in the cyber-security course. They are required to bring their laptops to class every day, and the course is conducted via the local (and Academy-wide) intranet wirelessly using those laptops. Some of the labs in the course require students to use a set of penetration testing programs that can probe for and exploit vulnerabilities in unpatched operating systems. Due to the sensitive nature of these applications and to prevent a security incident, it was necessary to establish a virtualized environment in which students could work. The following is a description of that system, which supported six sections of the class at the same time (but could have supported more, if needed).

A wireless router is attached to the ceiling of each classroom and connects student laptops to the system shown in Figure 1. The classroom routers are connected via Ethernet to a 1000 Mbps Catalyst 4507 switch. The switch has connections to both the ESX server (more to follow about the server shortly) and the USNA intranet, allowing students to access classroom items, notes, and other online resources, while also providing students access to the virtual sandbox environment via the VMware *Vsphere*TM client software on their laptops. *Vsphere*TM is a virtualization platform for building cloud infrastructures [8].

When connected to the virtual environment via the *Vsphere*TM client, students are only capable of utilizing resources and accessing other virtual machines (VMs) within the virtualized network. In order to handle the load imposed by 126 concurrent users (six classrooms of twenty students each and their instructors), a four-server system was installed as indicated in the center of Figure 1. Three of the servers are ESX virtualization servers, while the fourth is the vCenterTM server—providing administrative control over the virtualized environment. At the end of each class period, the instructor could quickly and easily restore the virtualized environment to the original settings for the next class. Each server is connected via a Catalyst 3560 switch to a Dell EqualLogic PS4000X SAN 9.6 TB disk for storage. Server specifications are itemized below and the classroom connectivity to the server is depicted in Figure 1.

- ESX Server Specifications:
 - DELL PowerEdge R710
 - 6-core Intel Xeon 5645 2.4GHz, 128GB RAM, 600GB disk
 - 2 × quad-port gigabit NIC
- vCenterTM Server Specifications:
 - DELL PowerEdge R210II
 - quad-core Intel Xeon E3-1270 3.4GHz, 8GB RAM, 600GB disk

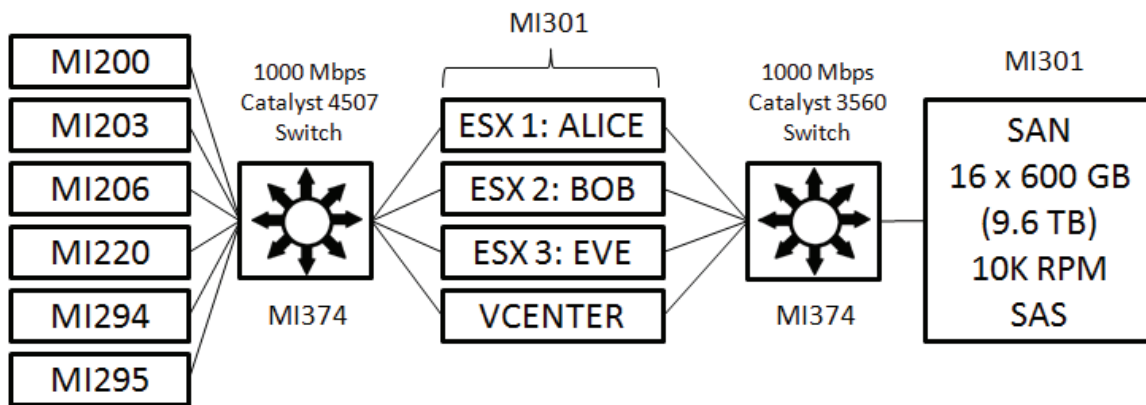


Figure 1. Topographical view of classroom wireless network connectivity to the ESX server system, where the six classroom wireless routers are labeled MI2XY on the left-hand side, a numbering scheme associated with the cyber security classroom/lab on the second floor in Michelson Hall (MI) of the U. S. Naval Academy.

To support the wired- and wireless-networking labs, in which the students build networks of both types, each classroom is outfitted with a 4' x 2' storage cart containing CAT5 patch cables, power strips, extension cords, a 1000 Mbps switch, an 8-port 100 Mbps router, as well as several 802.11n WAPs and 5-port 100 Mbps switches.

In addition, in order to support a lab involving the disassembly and reassembly of a modern PC, we acquired approximately 60 old PCs and LCD monitors from recent USNA graduates who no longer wanted their four year old machines. Students in the cyber security course use these machines during a lab where they disassemble, then reassemble a PC, with a focus on learning the names and functionality of various major architectural components.

4.2 Software Setup

This section covers student and server software used in the course. We begin by looking at the student software. All the software required for the cyber-security course was bundled into one installation file and provided to students at the beginning of the semester. A total of 180 licenses (this is sufficient to handle the number of students in a class, across all sections, at one time) were purchased for the Vsphere™ software used to interface with the vCenter™ server. All other programs were procured free of charge from the Internet or were written by USNA faculty. Software included in the installer is as follows:

- Text editors:
 - Binted—A binary-text editor.
 - Frhed—A hexadecimal editor.
 - Notepad++.
- Browsers:
 - Google Chrome installer.
 - Firefox setup installer.
- Network utilities:
 - Netcat.
 - WinSCP.
 - PuTTY.
 - OpenSSL (Win32).
- Encryption and forensics tools:
 - AES—A java application for AES encryption.
 - MD5—A hash generator.
 - Scalpel—A free tool for file carving.

- Other software:
 - VMware vSphere™ 4 Enterprise Plus client installer.
- Data files (text and image):
 - Various example files used during the forensics lab.

Note that other software which students used throughout the course, such as the JavaScript interpreter, encryption programs, demos, and so on, were made available via the course website. If new versions of software were needed to replace the ones originally installed, these too were made available via a hyperlink from the course website.

We now turn our attention to the server software. The VMware vCenter™ server runs on Microsoft Windows™ Server 2008. Within vCenter™, the virtual environment is logically segregated by classroom, where each folder contains all the VMs necessary to create the virtual network utilized by one class of students. Virtual-machine images were created for instructors, students, routers, and target VMs, which were then duplicated as needed. All the VMs comprising one classroom's worth of hosts were copied into a given classroom folder, then configured to the desired topology. Student and instructor VMs were built on Backtrack 5, while the VMs designed for students to attack and defend during the final labs of the class include Linux 2.6.x machines, Windows™ XP Pro 2002 workstations, and Windows™ Server 2003 hosts. Routers were implemented within the virtual space using Vyatta Core, open-source software. Within each class, VMs were organized into four separate networks: two for student teams, one for the instructor virtual machine, and one neutral network (a symbolic placeholder for the Internet).

4.3 Student Laptops

The Naval Academy acquires and configures the laptops that Midshipmen are required to purchase, independent of the cyber-security course. Requirements and specifications for the laptops for the class of 2015 were determined, in part, by the cyber-security course developers. The laptops were required to be relatively affordable, easily carried to and from the classroom, sufficiently fast to prevent obsolescence prior to the completion of a student's four-year undergraduate education, and capable of running via battery through a two-hour lab. The following is a listing of the laptop's specifications:

- System: Lenovo ThinkPad T420 Laptop
- Memory: 4GB

- Hard Drive: 320GB SATA
- DVD-ROM Drive: SATA 8X DVD Multi-Burner
- Ethernet: Intel 82579LM Gigabit Ethernet
- Wireless LAN: 802.11a/b/g/n Intel Centrino Advance-N 6205
- Operating System: MS Windows™ 7 SP1 Enterprise
- Power: 9-cell battery and AC adapter

The only peripheral required but not standard on any modern laptop was a Common Access Card (CAC) reader—allowing students to examine the certificate residing on their CAC (which is also issued to each student) as part of a lab activity, and allows them to access secure Department of Defense websites.

4.4 Lessons Learned

While there was sufficient time during the semester to configure and test the virtual environment upon which the final labs in the course depend, the same could not be said of the network infrastructure on the first day of the course. When students arrived for their first lecture, they were instructed to download and run the course's software installer. It became immediately apparent that the architecture could not withstand 120 students wirelessly downloading a 300MB file (hosted on the production servers) all at once. Most students needed to cancel the download and reattempt from their room later that night when there was less network traffic on the system. To resolve this issue in future semesters, we broke the installation program into three smaller pieces, and that has already proven, for the spring semester, to have resolved this problem.

5. FINDING AND DEVELOPING INSTRUCTORS

5.1 Instructors and Their Diversity

As noted, there was only six months lead time between the determination being made to deliver the cyber-security course and the start of the fall 2011 semester. Finding and hiring enough new faculty members (whether part-time or full-time) with appropriate qualifications to teach cyber security in this timeframe was a difficult proposition. For this reason, interested faculty members were sought from other USNA departments, from the campus IT staff, and also from outside of the USNA academic community. In all, there were a total of 16 instructors, from a variety of USNA departments, who taught during the inaugural semester of the cyber-security course. Some faculty members were active military officers who brought a great deal of relevant operational exposure gained during their previous career assignments.

5.2 Charm School

Although each of the instructors possessed a technical background, few were familiar with all of the course material, and none were experienced in teaching (or conducting research in) cyber-security. To prepare the instructors, a two-week, full-time “teach the teachers” class was offered three weeks prior to the beginning of the fall 2011 semester. Affectionately known as “Charm School”, the goal of this instruction was to cover all 41 lectures and labs of this first-year course in only two weeks. Led by the Course Coordinator, 12 of the 15 instructors were able to participate in this training. All found the experience worthwhile. Charm School also served as a means to “shake-out” the course, identifying better ways of teaching some material, as well as correcting some of the “bugs” in various course resources.

5.3 Lessons Learned

Weekly instructor meetings, an instructor only course website, and instructor-email lists supported instructor communication and knowledge sharing. Although lessons were available on the instructor website, the weekly meetings served as an open forum for instructors to relate important experiences and to ask questions. These meetings also helped to ensure consistency in the delivery of the material. The lessons on the course website provided examples and in-class demonstrations. Instructor meetings were often used to test these demonstrations to ensure maximum usability in class. However, testing does not always uncover every issue; a classroom full of curious students is usually able to find a problem if there is one! Instructor-email lists served as a means to relay valuable near real-time information to communicate fixes and alternatives. Labs and demonstrations were tested by instructors prior to classes, and for the most part they worked as expected. Of the few failures noted, most were due to numerous students attempting to perform the same activity at once and overloading the host system.

We were extremely fortunate that all of our instructors were able to teach the entire course without need for any emergency replacements. If possible, it would be good to build in a little redundancy in terms of the teaching staff to cover any potential loss of personnel. Our instructor-email list was particularly useful for coordinating substitutes, and for coordinating make-up labs, so that only one make-up lab needed to be scheduled for all students who missed a given lab.

6. BUDGETING

6.1 Classroom and Support Infrastructure Costs

The technical and hands-on format for the course necessitated the immediate need for properly outfitted labs to teach the course, and USNA embarked on a process to convert existing classrooms to accommodate this. The new requirement for first-year students to purchase laptops instead of desktops facilitated the movement to a wireless classroom/lab at a greatly reduced cost to USNA, allowed the students to have their own personal machine for hands-on activities and facilitated wireless networking exercises. Taking advantage of the fact that all students had laptops, six classrooms were converted to support the cyber-security course. These classrooms were already outfitted with an instructor station including computer and projection system. The major addition to the six classrooms was a wireless access point (WAP) and dedicated equipment purchased to support network-based exercises. A breakdown of the equipment is found in Table 1.

Table 1. Summary of the equipment and costs to support six classrooms where we taught the cyber-security class.

Item	Cost	Quantity	Total Cost
5 Port Switch	\$20.00	36	\$720.00
24 Port Switch	\$170.00	6	\$1,020.00
Wireless-Access Point	\$130.00	36	\$4,680.00
Ethernet CAT5e (10 ft)	\$3.00	156	\$468.00
Ethernet CAT53 (25 ft)	\$17.00	18	\$306.00
TOTAL			\$7,194.00

Given the nature of the material and exercises as previously discussed, a conscious decision was made to have the students work, experiment, and practice in a virtual environment that was fully separated from the Internet and USNA's Intranet. USNA designed an independent server cluster—production server, test-bed (sandbox) server, and associated software (see Section 5). The approximate cost for this equipment, software, and teaching aids was \$220,000. This coupled with the equipment shown in Table 1 resulted in a total cost of equipment and software of roughly $\$220,000 + \$7,194 = \$227,194$.

6.2 Manpower Costs

Manpower presented an entirely different issue. Given the six month timeframe, the demand for qualified staff (approximately 30 sections of 20 students each) could not be budgeted for using traditional methods. Fortunately, USNA has a strong STEM emphasis, and faculty from the Math and Science and the Engineering and Weapons Divisions joined together to cover nearly all of the sections, with adjunct instructors being employed to back fill in courses from the home departments of the faculty who volunteered to teach for us. The cost to employ adjuncts was approximately \$100,000 per semester, and that cost is anticipated to decrease as full-time faculty members are hired in support of the cyber program. Additionally, given the technical nature of the course and the extensive network infrastructure used, technical-support staff will be increased by two technicians.

6.3 Lessons Learned

Given the short lead time for rolling out the cyber-security course, we needed to remain flexible with the budgeting. We found that by using existing faculty to teach the cyber course and providing development support for them (for example, the website and Charm School), we could rather easily find adjunct faculty to instruct in disciplines with less market demand in our region. In the end, we found that in this first year, the costs of personnel and equipment were about the same.

7. RECOMMENDATIONS

The USNA decision to require all first-year students in the Class of 2015 to take an introductory core course in cyber security was a major academic undertaking that required a highly coordinated effort by a wide range of faculty and staff at USNA. The course rollout received much media attention [1-2, 4-5] and, according to our measures, was highly successful.

The key lessons learned when designing the curriculum were to incorporate multiple hands-on activities throughout, be selective and repetitive, to reiterate and reuse techniques, concepts, and tools, to ask students to understand and modify basic programs rather than write code of their own, and to pursue just a handful of topics in depth. Due to the use of a website to deliver course material, the purchase of a textbook was not necessary. With respect to developing instructors for the course, the "Charm School" was essential in cultivating quality instructors and ensuring all were working with the same material. The multiple forms of communication utilized were vital to the success of the course.

Regarding the hardware and software logistics of the course, advanced research and planning is critical, as is having the appropriate amount of time needed to configure and to test

systems in advance of delivering the actual course. A lot of time and energy was spent developing instructors, and perhaps doing this in house was more cost effective than hiring outside instructors.

A more formal mechanism for capturing instructor feedback on the course would have been useful allowing us to better track suggestions for improvement. Although we conducted surveys to obtain student feedback, more formal assessment measures were needed during course delivery to fully ascertain whether learning objectives were being met as was done in computer literacy courses taught in Maryland state universities and community colleges [3].

Our goal has been to make the insights that we gained in developing our first-year, cyber-security course available to those thinking of implementing a core course and in particular a course in cyber security. The challenges are great, and it will take a team effort to be successful. But, the rewards are great in that cyber security is an important domain for all to be more versed in and cyberspace is safer when all users practice good habits and demonstrate awareness.

8. REFERENCES

- [1] Brown, M. H. 2011. Naval Academy Preparing Officers for Cyberwarfare. Baltimore Sun. DOI=<http://www.baltimoresun.com/news/maryland/education/bs-md-naval-academy-cyber-security-20111019,0,2371754.story>.
- [2] Carroll, C. 2011. Cyberwarfare Joins the Curriculum at Service Academies. Stars and Stripes. DOI=<http://www.stripes.com/news/cyberwarfare-joins-the-curriculum-at-service-academies-1.158642>.
- [3] Kaza, S., Taylor, B., and Turner, C. 2011. Security in Computer Literacy-A Model for Design, Dissemination, and Assessment. In *Proceedings of the 42nd ACM Technical Symposium on Computer Science Education* (Dallas, Texas, USA, March 9–12, 2011), SIGSCE'11. ACM, New York, NY. DOI=<http://dl.acm.org/citation.cfm?id=1953174>.
- [4] Montalbano, E. 2011. Navy Adds Cybersecurity Academy Requirements. DOI=<http://www.informationweek.com/news/government/security/229300570>.
- [5] Naval Academy to Add Cyber-Security Classes. DOI=<http://thedailyrecord.com/2011/03/07/naval-academy-to-add-cybersecurity-classes/>.
- [6] Needham, D. and Vincent, P. Initial Report of the Dean's Cyber Warfare Ad Hoc Committee, USNA-CS-TR-2011-02. U.S. Naval Academy Computer Science Department, Annapolis, MD, 2011
- [7] President's Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, May 2009. DOI=http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
- [8] VMware Vsphere™ for Enterprise. DOI=<http://www.vmware.com/products/vsphere/mid-size-and-enterprise-business/overview.html>.