Building a Successful Cyber-security Program

David Dampier
Distributed Analytics and Security Institute
Mississippi State University
Box 9627, HPC A129
Mississippi State, MS 39762-9627
001-662-325-0779
dampier@dasi.msstate.edu

ABSTRACT
Many institutions today are interested in starting cyber-security programs. It is one of the hottest topics out there, and an increasing number of students are interested in studying cyber-security. This paper describes a recipe that can be used to build a successful cyber-security program, either from scratch or from a minimal capability that already exists. The essential elements that must be acquired and developed to build the program along with concrete examples from an existing successful program are provided. The paper also talks about why it may be a good idea to build this program, including some of the benefits of having a quality cyber-security program, including scholarships to attract quality students.

Categories and Subject Descriptors
K.3.0 [Computers and Education]: Cyber-security Education

General Terms
Security.

Keywords
Cyber-security, CAE, Education.

1. INTRODUCTION
Cyber-security is a very hot topic, and appears to only be increasing in popularity in the foreseeable future. An increasing number of potential students are interested in pursuing careers in cyber-security, and that is because there are an increasing number of job opportunities predicted into the future. Funding priorities at all levels have made cyber-security a hot research area as well. This raises the interest of administrations at research institutions where funded research pays the bills. More universities now than ever before seem to want to build cyber-security programs to take advantage of the increased interest among students and funding agencies. This paper describes what the author believes to be the essential properties that an institution needs to build a successful cyber-security program, for education and/or research. In the following sections, we will discuss the essential elements to building a successful cyber-security program with specific examples from a very successful program.

Conference'10, Month 1–2, 2010, City, State, Country.

2. ESSENTIAL ELEMENTS
In order for an institution to build a successful cyber-security program, it is essential that they develop capabilities in six areas. These six areas are: faculty, courses, equipment and laboratories, students, budget, and credentials.

2.1 Faculty
To build a successful cyber-security program, an institution must have faculty that are qualified and interested in the subject matter, and those faculty should be in a range of disciplines, and and varying experience levels. It would be difficult to quickly develop a national reputation for cyber-security if only junior faculty are hired and expected to do it by themselves. New faculty need to be mentored by more senior faculty who already have experience and a reputation for doing good work. Hiring at least some faculty that are more experienced will have a quicker impact on the stature of the institution's cyber-security program.

Faculty are also needed across multiple disciplines. Faculty are needed in computer science (CS), computer engineering (CPE), and information systems (IS) at a minimum, but for a more robust program, an institution would want to develop faculty in other engineering disciplines as well, especially electrical engineering and industrial engineering. Technically capable people in CS and CPE, are needed to satisfy the requirements for building hard-core cyber-security programs. IS people are needed to make sure that the program sufficiently covers policy, legal, and management issues. If the programs are to include systems development, especially control systems engineers, then EE and ISE are also desirable.

Faculty are not only needed across all of these disciplines, but in sufficient quantity to build and teach classes, propose and conduct research, and mentor students and junior faculty. They must also be of sufficient quality to successfully publish and build the reputation of the institution, be able to write successful grant proposals to bring in much needed funding, guide graduate students in meaningful research, and provide leadership for the growing cyber-security program.

At Mississippi State University (MSU), there are currently eight dedicated cyber-security faculty, across three primary disciplines: computer science, electrical and computer engineering, and information systems. Three are full professors, three are associate professors, and two are assistant professors. Additionally, through cyber-security research, additional faculty from these disciplines, as well as industrial engineering collaborate on active research projects.

2.2 Courses

Once faculty are in place, courses must be developed that cover the critical disciplines that are involved in cyber-security. These courses include material from many different disciplines:

- Security Policy and Law
- Computer Security, including both Hardware and Software
- Network Security
- Digital Forensics
- Cyber Physical Systems Security, often referred to as SCADA Security

Courses need to provide a well-rounded education to prepare the students for all levels of cyber-security work. The National Initiative for Cyber-security Education (NICE) was developed at the National Institute of Standards and Technology to provide guidance for cyber-security education from K-12 to graduate education. The NICE Framework (see Figure 1) contains a set of categories that describe work tasks in cyber-security so that the right skills are developed in personnel that will work across the spectrum of cyber-security. Each of these categories is broken down into knowledge units that personnel in that category need to be proficient in.

Needed courses educate to these knowledge units and build on basic knowledge in the disciplines described in Section 2.1. For example, in computer science or computer engineering, courses would build on a basic understanding of computational science and engineering such as programming, systems programming, networking, etc.

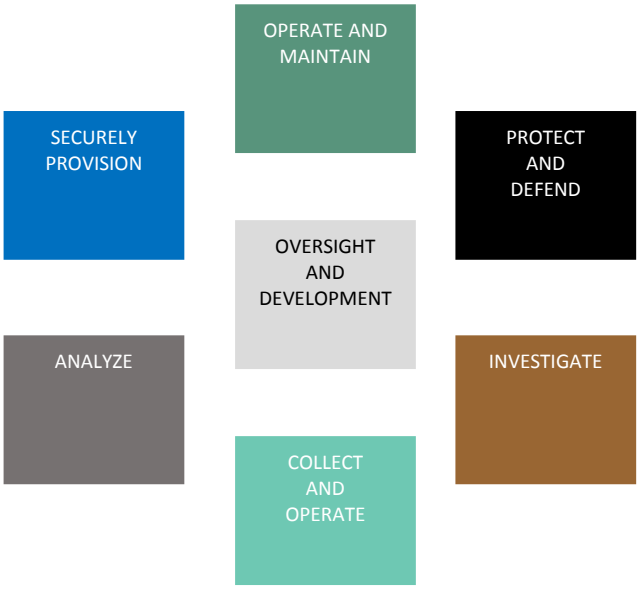

Figure 1. NICE Framework[1]

- SECURELY PROVISION
  Includes specialty areas responsible for some aspect of system development, i.e., conceptualizing, designing, and building secure IT systems.

- OPERATE AND MAINTAIN
  Includes specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.

- PROTECT AND DEFEND
  Includes specialty areas responsible for identification, analysis, and mitigation of threats to internal IT systems or networks.

- INVESTIGATE
  Includes specialty areas responsible for investigation of cyber events and/or crimes of information technology (IT) systems, networks, and digital evidence.

- COLLECT AND OPERATE
  Includes specialty areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

- ANALYZE
  Includes specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

- OVERSIGHT AND DEVELOPMENT
  Includes specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.

Early in the development of the program, courses can be cross-disciplinary, but as the depth of the program grows, the amount of material to cover will grow and require courses to be much more specialized.

At MSU, there are five permanent courses over three departments that are offered at least once per year, and since 2008, eleven different special topics classes have been offered, many multiple times. At least two special topics classes are offered each academic year.

2.3 Equipment and Laboratories

As with all technology based education, it is better if classroom instruction is supplemented with what is sometimes called "Discovery Learning." [1, 2] This is certainly the case with cyber-security education. Hands-on instruction is critical to building a quality cyber-security education program, and this requires laboratory facilities. Laboratory facilities should be of sufficient quantity and quality to support the expected size of the program, and the different disciplines represented in the program.

In a general cyber-security lab, it is recommended that there are as many machines as space will allow. They should be networked

[1] http://crsc.nist.gov/NICE/framework, downloaded on March 17, 2015.

together, but isolated from the internet. This allows the students to do things that if connected to the internet may prove embarrassing to the institution. Students should be allowed to do anything they want that will not cause harm to others, so there should be a mechanism to rewrite the disk images on a nightly basis. If an internet capable machine is present in the room, it should be isolated from the student network, so that students cannot accidentally upload bad things to the internet. Machines should also be set up to boot in Windows and Linux, or at the least have VM capability to run Windows and Linux virtual machines.

It is also essential that hardware be kept up to date and refreshed as often as possible. This will require a budget. One way to offset this cost is to charge a lab fee on courses that use the lab. This will provide much needed funds to keep the lab refreshed.

Software must also be provided that is sufficient to allow students a realistic experience. Whether it is commercial or open source is not really important, but students should be exposed to as many different software tools as possible for a thorough education. If physical laboratories and/or hardware are not possible given the budget, then using virtual laboratories like those available in the RAVE[2] program is acceptable. Although virtual experiences are not as good as hands-on physical experiences, they are sufficient.

At MSU, there are three physical laboratories used for cyber-security:

- Cyber-security Lab: 22 networked workstations running Windows, Linux, and MacOS. Machines are isolated from the internet and a Ghost® server maintains the integrity of the machines in the lab.
- Digital Forensics Lab: 20 forensics workstations with most of the commercial and open-source software available for digital forensics. The lab also contains multiple units for cell phone analysis, remote disk imaging, write-blockers, and adapters for every conceivable media type so that students can get exposure to anything that they may see in the field.
- Cyber Physical Systems Lab: Seven workstations representing seven different critical infrastructures with real-world hardware and software to operate the systems. Figure 2 shows a picture of the laboratory and all seven workstations:
  - Gas Pipeline
  - Water Storage Tank
  - Ground Liquid Storage Tank
  - Warehouse Conveyor System
  - Industrial Blower
  - Steel Roller System
  - Chemical Mixing Station

MSU also hosts one of the RAVE servers that are available for use by institutions that cannot afford a physical laboratory.

2.4 Students

Getting students to study cyber-security and building a successful cyber-security program is sort of a “chicken and egg” problem. In order to attract good students to a program, they have to be convinced that it is worth the investment of their time and resources, but to have a world-class program, that program has to have good students. In cyber-security, motivated students are needed that are willing to do what it takes to learn cyber-security and focus their education on it. This is the only way to build a successful program. Students have to graduate and go to work in the industry and be exceptional in their performance to get the program they graduated from noticed and recognized as a quality program. But, in order to get students, a relatively good program has to exist.

Figure 2: Cyber Physical Systems Laboratory at MSU

For students who want to study cyber-security, one or two courses is not enough to keep them motivated. There needs to be at least 12-15 hours of coursework taken throughout their program of study. This is the only way that they will get all of the material needed to be qualified to work in cyber-security.

Another issue is that American citizens are desirable for students in cyber-security. The biggest employer of cyber-security graduates right now is the federal government, and in order to get hired by the federal government, the student has to be a citizen. One of the benefits of having a quality cyber-security program is that not only will the program attract high-quality students, more American students will likely stay around for graduate school and conduct research in cyber-security. The CyberCorps: Scholarship for Service® (SFS) program, which will be discussed later in the paper, is a great motivator to convince good undergraduate students to stay for graduate school, thereby increasing the number of American citizens enrolled in the program. Jobs are available in the government and private industry to graduates at all levels, but the best way to increase American graduate students is to grow them in undergraduate programs.

At MSU, in large part through the availability of the CyberCorps scholarships, the percentage of graduate students in the associated degree programs that are Americans has increased substantially. In computer science, the primary major associated with the cyber-security program, American citizens make up 63% of the graduate student population.

2.5 Budget

Having faculty, building courses and laboratories, and attracting students are certainly important factors in building a successful

[2] See https://redmine.rave-lab.com/projects/rave-lab/wiki

program, but they cannot be done without funding. New programs cost money, and a commitment of at least some funding needs to be made by the institution to build and maintain a successful program. In order to maximize effectiveness, funding should be provided for faculty lines dedicated to cyber-security, assistantships and scholarships for cyber-security, and laboratories and equipment for the physical labs required. Faculty lines should be dedicated to cyber-security across multiple disciplines, according to the list of topics that are required to establish the program. An infusion of funding to establish initial assistantships or scholarships for students until a reputation can be established to attract external funding will likely be necessary to allow for time to build. Laboratories and equipment, as well as new course preparation time cost money, and unless the administration is committed to making the required investment, it is going to be difficult to make the leap to a successful program in a reasonable amount of time. There are grant opportunities that are available for capacity building, but there usually has to be at least a minimal program in place to demonstrate the potential for excellence and attract capacity building funding.

2.6 Credentials

If a school wants to be recognized as a leader in cyber security, they must develop breadth and depth in cyber-security. Breadth of capability will help bring good students to the program, and depth of capability will produce better graduates. To demonstrate this breadth and depth, an institution is best positioned if they can establish a level of excellence in the field, and can demonstrate that by qualifying for one of the DOD/DHS Center of Academic Excellence programs. These programs include:

- CAE-2Y: Center of Academic Excellence in Information Assurance/Cyber Defense Education for Community Colleges and 2 year technical schools
- CAE-IA/CD: Center of Academic Excellence in Information Assurance/Cyber Defense Education for four-year institutions
- CAE-R: CAE in Information Assurance/Cyber Defense Research for research universities
- CAE-Cyber: Center of Academic Excellence in Cyber Operations for schools with a very advanced technical capability, and an ability to educate future cyber warriors

2.6.1 CAE-2Y

The CAE-2Y credential, sponsored by the Department of Homeland Security and the Department of Defense was designed to recognize community colleges and 2 year technical schools that have achieved a level of excellence in cyber-security education. It was recognized by the federal government that not all jobs associated with cyber-security require a four-year college degree, and that there were a significant number of community college graduates that could fill those jobs. Schools qualifying for the CAE-2Y credential must satisfy a set of rigorous criteria and map their courseware to an extensive set of core Knowledge Units:

- Basic Data Analysis
- Basic Scripting
- Cyber Defense
- Cyber Threats
- Fundamental Security Design Principles
- Information Assurance Fundamentals
- Introduction to Cryptography
- Information Technology System Components
- Networking Concepts
- Policy: Legal, Ethics, and Compliance
- Systems Administration

CAE-2Y institutions must also map their courseware to at least one optional Knowledge Unit. A list of optional KUs is too lengthy to mention in this paper, but may be found on the internet[3]. As of 2014, there are currently 32 institutions that have successfully achieved the CAE-2Y credential.

2.6.2 CAE-IA/CD

The CAE-IA/CD credential, sponsored by the Department of Homeland Security and The Department of Defense was designed to recognize four year schools that have achieved a level of excellence in Information Assurance and Cyber Defense Education. Originally known as the CAE-IAE (Information Assurance Education), the credential was based on a set of federal standards established by the Committee on National Security Standards (CNSS). The primary standard was NSTISSI-4011: National Training Standard for Information Systems Security (INFOSEC) Professionals[4]. The CAE-IAE credential is the oldest and most basic of the CAE credentials for four-year institutions, started in 2000.

To currently achieve this designation, an institution's curriculum must conform to a rigorous set of criteria and be mapped to a detailed set of knowledge units:

- All of the CAE-2Y core Knowledge Units, plus:
- Databases
- Network Defense
- Networking Technology and Protocols
- Operating Systems concepts
- Probability and Statistics
- Programming

CAE-IA/CD applicants must also map their courseware to at least two optional Knowledge Units. A list of optional KUs may be found on the internet[3]. Building the application package for this credential is a very time-intensive process (probably at least 100 man-hours for someone very familiar with the curriculum). There are currently 130 institutions that have achieved either the CAE-IAE credential and/or the CAE-IA/CD credential. Current CAE-IAE schools are in the process of applying for recognition as a CAE-IA/CD. They have until the end of their current designation period, or they will lose their designation.

2.6.3 CAE-R

The CAE-R credential, sponsored by the Department of Homeland Security and The Department of Defense was designed to recognize research universities. It is a more advanced credential designed to recognize schools that contribute materially to the science of cyber-security. Originally started in 2008, only universities that grant doctoral degrees are eligible, with the

---

[3]https://www.iad.gov/NIETP/documents/Requirements/CAE_IA-CD_KU.pdf

[4]https://www.cnss.gov/CNSS/openDoc.cfm?L1x07KUpISkYvaHDKM5oMA==, downloaded March 19, 2015.

exception of the military service academies. To qualify, the institution must show a strong record of research in cyber-security related topics. This is demonstrated through a set of criteria that includes the number of doctorates granted in the last five years (the minimum is three), the number of faculty, research grants awarded to the institution, and research publications by both faculty and students. Publication minimums are established that include at least ten research publications by faculty and students over the course of the previous five years. All of this evidence must be related to cyber-security. There are currently 58 institutions that have achieved this credential. Of those 58, 38 also have the education credential.

MSU was one of the first institutions recognized as a CAE-R in 2008. MSU, for example, awarded 14 PhDs to graduates conducting research in cyber-security between 2008 and 2014. Publications in cyber-security related topics number in the 70s for faculty and over 20 for students in the same time period.

2.6.4 CAE-CYBER

The CAE-Cyber Operations credential is the most exclusive of the CAE credentials. It is sponsored by the Department of Defense only, and is designed primarily to produce cyber operators for the various cyber command units. This credential requires very specialized instruction, and that instruction has to be very well documented. Part of the CAE-Cyber evaluation is a site visit by representatives of the DOD to verify that the institution really does what it says it does in the application. The elements of the required education are outlined in very specific knowledge units. The details of how those knowledge units are achieved is documented in an application submitted for review. An initial review of applications results in a short list of institutions to be visited. The number of schools to be approved is expected to be very low each year, with the maximum number to be recognized not many more than 20. In the first three years, only 13 schools have been awarded this credential.

It is likely that only computer engineering or computer science programs will qualify, unless a new cyber operations degree program is designed specifically for the credential. With this credential, students should be U.S. citizens as they are all likely destined for employment with the Department of Defense (if they desire). Another aspect of this program is that all students at these institutions are eligible to participate in summer training opportunities in the techniques taught in the program. Many students will be given the opportunity to gain a security clearance well before graduation in order to participate in the summer training, much of which is classified.

At MSU, qualification in cyber-operations is achieved through a graduate certificate program associated with the MS or PhD in computer science. The MSU program was awarded this credential in 2013.

3. BENEFITS OF A QUALITY CYBER-SECURITY PROGRAM

So, what is the return on investment (ROI) for doing all of the things described above? Some would say that there is no guaranteed ROI, at least from the credentials part. We would argue that is not the case. Making the financial investment to attract quality faculty, build the necessary courses, build appropriate laboratories, recruit motivated students, and go through the significant work of applying for the CAE credentials will reap some benefit, if it is done seriously. Students will hear about the institution, and they will come. Cyber-security is a very popular job title now and into the future. A concrete example of making this investment is described in the next section, and that is the ability to compete for scholarship programs that are available only to institutions with quality programs. The next section will describe this scholarship program.

4. CYBERCORPS: SCHOLARSHIP FOR SERVICE® (SFS)

Achieving one of the last three credentials makes an institution eligible to apply for the SFS program. This program is a National Science Foundation funded program that provides capacity building grants as well as scholarship grants. These scholarship grants are then used to give scholarships to students in the following categories:

- Undergraduates, junior and above, for up to two years.
- 5 year BS/MS candidates, junior and above, for up to three years.
- MS candidates for up to two years.
- PhD candidates for up to three years.

A list of current schools that have active SFS scholarship programs is shown in Table 1.

MSU has had an active SFS program since 2001, and is currently operating on their fourth SFS grant. Approximately 150 students have benefitted from the SFS at MSU.

4.1 Benefits of SFS

Students awarded the SFS get a full ride for the period of time allotted to the scholarship. They receive the following benefits:

- Full Tuition and Fees for Students
  - Out of State and In-State
- Book Allowance – up to $1000 per year
- Health Insurance Allowance – up to $2000 per year
- Travel Allowance – up to $3500 per year
- Stipend
  - Undergraduates: $10,000 per semester
  - Graduates: $16,000 per semester
- Summer Internship, preferably paid

4.2 Obligations Incurred with SFS

Students awarded the SFS incur an obligation to serve the government as a cyber-security professional after they graduate. This obligation is one year of service for every year (or partial year) of scholarship. This obligation can be fulfilled through service for one of the following:

- Local, State, or Federal Government
  - State universities count as state government, especially for payback for PhD graduates
- FFRDC (National Labs, Mitre, IDA, TVA, etc.)
- Tribal Governments

Table 1. Schools with SFS Programs[5]

Air Force Institute of Technology	Idaho State University	New York University	SUNY-Buffalo	University of North Carolina-Charlotte
Arizona State University	Indiana University of Pennsylvania	Norfolk State University	University of Alabama-Huntsville	University of North Texas
Auburn University	Iowa State University	North Carolina A&T University	University of Arizona	University of Pittsburgh
Cal State University-Sacramento	James Madison University	Northeastern University	University of California-Irvine	University of South Alabama
Cal State University-San Bernardino	Johns Hopkins University	Norwich University	University of Houston	University of Texas- Austin
Carnegie Mellon University	Kansas State University	Pace University	University of Idaho	University of Texas-Dallas
Dakota State University	Marymount University	Pennsylvania State Universit5y	University of Illinois Chicago	University of Texas- San Antonio
Florida State University	Mississippi State University	Purdue University	University of Illinois Urbana-Champagne	University of Tulsa
George Washington University	Missouri S&T	Stevens Institute of Technology	University of Maryland-Baltimore County	University of Washington
Georgia Institute of Technology	Naval Postgraduate School	Syracuse University	University of Nebraska-Omaha	Virginia Polytechnic Institute
Hampton University	New Mexico Institute of Mining and Technology	Towson University	University of New Mexico	

Additionally, the student must be able to obtain a security clearance appropriate for the job secured. They must perform an internship each summer that they are on the scholarship. This internship obligation does not extend to students pursuing a PhD on the scholarship. They are also required to attend a centralized job fair help each year by the Office of Personnel Management. They are permitted to fulfill these last two obligations through research performed at the respective institution, and academic job searching. Additionally, SFS scholars are obligated to search for employment that is appropriate for payback, and report their job searching activities on a website managed by the Office of Personnel Management. Failure to find a job within a reasonable period of time could result in a debt to the government to pay back the money provided for their education. It is also important to note here that collection of these student debts is the responsibility of the granted institution, and that money has to be returned to the U.S. Treasury.

5. CONCLUSION

This paper has described a path to building a successful cyber-security program, with examples of how one institution, Mississippi State University built such a program over a period of over 15 years. That path included essential ingredients, including faculty, courses, equipment and laboratories, students, budgets, and possible credentials. The paper also described some of the benefits available to schools which satisfy those credential requirements.

6. REFERENCES

[1] Dampier, D. and Vaughn, R. 2009. Hands-On Discovery Learning in Computer Security and Forensics. In *Proceedings of the 2009 International Conference on Engineering Education and Research (ICEER)* (Seoul, Korea, August 25-28, 2009).

[2] Vaughn, R. and Dampier, D. 2009. A Discovery Learning Approach to Information Assurance Education, In *Proceedings of the 2009 Hawaii International Conference on the System Sciences, Minitrack on Digital Forensics* (Waikoloa, Hawaii, January 5-9, 2009).

[5] List of Schools with SFS programs taken from https://www.sfs.opm.gov/ContactsPI.aspx on March 14, 2015.