https://doi.org/10.48009/3_iis_2020_135-141

Issues in Information Systems
Volume 21, Issue 3, pp. 135-141, 2020

STARTING A CYBER SECURITY PROGRAM AT A UNIVERSITY: A CASE STUDY

Jason E. James, Indiana State University, jason.james@indstate.edu

ABSTRACT

Many institutions today are interested in starting cybersecurity programs mainly because the job market demand is very high students want to take advantage of the employment opportunities. This paper describes the journey that one university went through to build a successful cybersecurity program. There are essential components that must exist to build a successful program and this paper goes into what those are and describes specific examples from an existing successful program.

Keywords: Cybersecurity, CAE, Education

INTRODUCTION

Starting a new degree program or even modifying an existing program a college or university is no easy task. However, with the rapidly changing technology and dependence on IoT, we are experiencing a surge in cybercrime and digital threats. At the same time, the world is suffering from a severe lack of qualified and skilled professionals in cybersecurity positions (Dickens, 2018). According to a Cybersecurity Ventures, Cybercrime will more than triple the number of job openings to 3.5 million unfilled cybersecurity positions by 2021, and the cybersecurity unemployment rate will remain at zero percent (Morgan, 2018). With more students than ever attending college, why is this such an issue? And more importantly, how can we solve for it?

The cyber security industry getting more attention now than it ever has, and unfortunately, it's been long overdue. The cybersecurity workforce shortage has left CIOs, CSOs, and CISOs shorthanded and scrambling for talent while the cyberattacks are intensifying. Even though the salaries of cybersecurity positions are pretty high, many companies are having trouble filling cybersecurity positions because there are few professionals available to fill multiple open positions and even worse, there has been no one to educate them. That is, until now!

The field of cybersecurity has grown immensely with the proliferation of the Internet, and will likely only continue to expand well into the future. Indeed, cybersecurity focuses on strengthening the security and resilience of cyberspace, as described by the United States Department of Homeland Security, and involves a large array of vocations, including information security analysts, which the Bureau of Labor Statistics asserts will experience an 18 percent growth in employment by 2024, or a total of 14,800 additional jobs (Online Engineering, 2018).

Perhaps one of the most direct methods of beginning a career in the cybersecurity industry is to pursue a cybersecurity degree. In the midst of the cybersecurity employment crisis, the United States Government launched initiatives specifically for cyber security education that are designed to help schools develop the necessary degree programs. The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, developed a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development (Dickens, 2018).

In response to the cybersecurity job crisis and the United States Government initiatives, many colleges and universities have prepared to launch, or already started cybersecurity programs that includes certificates, associates, bachelors, masters, and even doctorates, that will allow students to obtain a degree in the field either on ground, totally online, or a combination of both.

An increasing number of potential students are interested in pursuing careers in cybersecurity, 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 cybersecurity programs to take advantage of the increased interest among students and funding agencies (Dampier, 2015). This paper describes

what the author believes to be the essential components, based on experience starting a cybersecurity program, that a higher education institution needs to build a successful cybersecurity program, for education and/or research. In the following sections, we will discuss the essential components to building a successful cybersecurity program with specific examples.

ESSENTIAL COMPONENTS

In order for an institution to build a successful cyber-security program, it is essential that they develop capabilities in six areas. These seven areas are: faculty, courses, credentials, students, CyberLab, service, and certifications.

Faculty

A successful cybersecurity program starts with qualified faculty. Cybersecurity programs need to have qualified faculty with varying industry experience, industry certifications, passionate in the subject matter, and have a broad range of disciplines. It would be difficult to develop a quality program and attract students if only entry level faculty are hired. Inexperienced faculty in the field of cybersecurity is good to have but they need to be mentored by more experienced faculty who have experience and the ability to develop cutting edge-curriculum.

A cybersecurity program needs faculty who are experienced and can teach across multiple disciplines. Faculty are needed in programming, security, forensics, computer science, information systems, information technology (hardware), networking at a minimum. Faculty should not only be technical, but also proficient in policy, legal, risk management, project management, and systems development to name a few. Faculty should be effective communicators, both oral and written, since they will have to develop and write course and teach those courses effectively.

Faculty are not only needed across all of these disciplines, but they will also be asked to build and teach classes, propose and conduct research, and mentor students. A successful cybersecurity program needs quality faculty to successfully publish and build the reputation of the institution, write successful grant proposals, direct graduate students in meaningful research, and provide leadership to grow and expand the cybersecurity program.

At XYZ University, there are currently seven dedicated cybersecurity faculty, across three primary disciplines: security, programming, forensics, information technology (hardware), and networking. Three are full time professors (one of which is the program director) and the rest are adjunct instructors. All of them multiple years of experience as well as industry experience.

Courses

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

- Security Governance, Policy, Law, and Ethics
- Security, including Network, Application, Physical, Computer, Information, Operational, Communication, End-user, and includes Business Continuity and Disaster Recovery
- Forensics, including Digital, Mobile, and Cloud
- Information Technology, including Hardware and Software as well as Information Systems
- Certification courses including

Courses need to provide a solid education to prepare students for a cybersecurity career. As discussed earlier, NICE was developed at NIST to provide guidance for cybersecurity education. The NICE Framework are categories that describe work tasks in cybersecurity in order for people to develop the knowledge, skills, and abilities that will be needed in the cybersecurity workforce and include common cybersecurity functions:

- Operate and Maintain
- Protect and Defend
- Investigate
- Collect and Operate

- Analyze
- Securely Provision
- Oversee and Govern

Each category of the NICE framework is further broken down into specific knowledge units that people need to know and understand and eventually become proficient.

The courses that are developed for a cybersecurity program need to provide the knowledge in these areas. The National Centers of Academic Excellence in Cyber Defense (CAE-CD) created knowledge units for the cybersecurity workforce that are complimentary in nature to the NICE framework. Higher education institutions that want to become CAE-CD certified then create courses that map to the CAE-CD knowledge units, which in turn indirectly map to the NICE framework, thus creating the education cybersecurity students need to enter the cybersecurity workforce.

Keep in mind, each of the CAE-CD and NICE Frameworks knowledge units were developed for different purposes, cybersecurity education vs. cybersecurity workforce, and the two are not a one for one relationship. However, many parallels and relationships exist between these two and even though the origin of the CAE-CD KUs and NICE Framework were developed for different reasons, they are complimentary in nature.

At XYZ University, the cybersecurity program courses were developed around the knowledge unit requirements for CAE-CD certification.

Credentials

If a higher education institution wants to be a leader in cybersecurity, they should strive to become a National Security Agency (NSA) and the Department of Homeland Security (DHS) National Centers of Academic Excellence in Cyber Defense (CAE-CDE) or Research (CAE-R) program.

While many cyber security jobs are open to students who attend any accredited cyber degree making sure a program is CAE designated can help to ensure students are studying cybersecurity concepts and practices deemed important by the federal government. Employers will know that graduates have studied a wide range of current cybersecurity tools in the field. While cybersecurity workers are in great demand regardless of where they go to school, there's a higher than average chance that students who go to a CAE program are ensured that they are learning the most valuable cybersecurity skills they can. While not attending a CAE-CD designated school is by no means a dead end to a student's future cybersecurity goals, it definitely increases the chance that students want to attend a CAE-CD school and obtain the best education to prepare them for the future cybersecurity workforce (Author Unknown, 2019).

In order to attract these future cybersecurity students, a higher education institution should position themselves in a higher a level of excellence and become certified (or qualified) to become a Center of Academic Excellence. The goal of the program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise. These programs include:

- CAE in CD Education (CAE CDE) for Associate, Bachelor, Masters and Doctoral Programs
- CAE in CD Research (CAE-R)
- CAE in Cyber Operations (CAE-CO)

All regionally accredited two-year, four-year, and graduate level institutions in the United States are eligible to apply to become a CAE-CD school. Prospective schools are designated after meeting stringent criteria, and may elect to specialize in several possible focus areas. CAE-CD institutions receive formal recognition from the U.S. Government for participating in the program. NSA and DHS do not provide funding to CAE schools but funding opportunities may be available from other sources such as the National Science Foundation.

NSA's CAE in Cyber Operations (CAE-CO) program supports the President's National Initiative for Cybersecurity Education (NICE): Building a Digital Nation, and furthers the goal to broaden the pool of skilled workers capable of supporting a cyber-secure nation. The CAE-CO program is a deeply technical, inter-disciplinary, higher education

program firmly grounded in the computer science, computer engineering, and/or electrical engineering disciplines, with extensive opportunities for hands-on applications via labs and exercises.

The CAE-CO program complements the existing CAE in Cyber Defense (CAE-CD) programs, providing a particular emphasis on technologies and techniques related to specialized cyber operations (e.g., collection, exploitation, and response), to enhance the national security posture of our Nation. These technologies and techniques are critical to intelligence, military and law enforcement organizations authorized to perform these specialized operations (NSA, 2019).

In order to achieve CAE-CDE, designation, a higher education institution's curriculum must conform to a rigorous set of criteria and be mapped to a detailed set of knowledge units that include requisite Foundational, Core (5 Technical or 5 Non-Technical), and Required Optional Knowledge Units (KUs) at either the Associate, Bachelor, Master, or Doctoral levels and demonstrate that a student can reasonably complete the necessary course of study to include all KUs identified.

Cybersecurity foundational KUs include three core areas that all higher education institutions courses must map to: Cybersecurity Foundations, Cybersecurity Principles, and IT Systems Components. In addition, a higher education institution can either map courses to a core of technical or non-technical requirements. The technical core KUs include basic scripting and programming, basic networking, network defense, basic cryptography, and operating system concepts. The non-technical core KUs include cyber threats, policy, legal, ethics, and compliance, security program management, security risk analysis, and cybersecurity planning and management.

In addition, a higher education institution must demonstrate program outreach and collaboration, center for CD education, a robust and active CAE-CDE academic program, CD multidisciplinary efforts, practice of CD at the institution level, and student and faculty CD efforts.

XYZ University, began preparation and approvals in November of 2017 and officially launched their cybersecurity program in Fall of 2018 with courses developed and mapped to the Technical core of KUs.

Students

Many students want to study cybersecurity and with so many institutions launching cybersecurity programs, building a quality, successful, well-known cybersecurity program is essential to market and attract students. XYZ University, launched their cybersecurity program in the Fall 2018 with 75 students and by Summer 2019, enrollments doubled.

A good cybersecurity program not only wants to be known as a world-class program but also has to attract and retain great students and therefore, students must feel it is worth the investment of their time and resources. The only way to build a successful cybersecurity program, motivated students are needed and are willing to do what is necessary to learn cybersecurity and become successful in the cybersecurity workforce. A good cybersecurity program needs to exist at higher education institution to have students graduate and work in the cybersecurity industry and be exceptional in their job and company in order to get their college/university noticed and recognized as a quality program.

A quality cybersecurity program needs more than just one or two courses at attract and retain students who want to study cyber-security. A quality cybersecurity program needs multiple cybersecurity courses, such as what the CAE-CDE recommends, taken throughout their program of study. In doing so, students will get all of the material needed to be qualified to work in cybersecurity (Dampier, 2015).

In order to succeed in a cybersecurity program, students should have problem-solving skills, technical abilities, attention to detail, oral and written communication skills, desire to learn, and multitask. Students in cybersecurity programs need the ability to work methodically (and in a detail-oriented way) and have abilities such as:

- Eagerness to dig into technical questions and examine them from all sides.
- Enthusiasm and a high degree of adaptability.
- Strong analytical and diagnostic skills.

In addition, soft skills are definitely highly desired such as:

- Excellent presentation and communications skills to effectively communicate with management and customers.
- Ability to clearly articulate complex concepts (both written and verbally).
- Ability, understanding, and usage of active listening skills (especially with customers!)

Finally, implementation skills and management skills can complement students with the aforementioned skills. Although, it is not a necessity to have all of these skills and characteristics, they make for a very successful student and then a very successful cybersecurity career (Author unknown, n.d.)

CyberLab

As with all technology-based education, good courses included not only classroom instruction but also hands-on learning. Cybersecurity education is no different. Hands-on learning is absolutely necessary to build a quality cybersecurity program, and this requires not only instructors who can teach it, but also courses designed to provide hands-on learning and using what is now being called a CyberLab facility. CyberLab classrooms should contain all the quality hardware and software necessary facilities to support the size of the cybersecurity program.

A CyberLab should contain as many computers as necessary based on the size of the program and expected class sizes and when possible other hardware such as servers. All computers should be networked together, but isolated from the Internet to allow students hands-on learning exercises that if connected to the Internet could do damage to a college/university reputation.

A CyberLab should allow students to do anything they can that will not cause harm to others. If an Internet connected computer is present in the CyberLab, it needs to be isolated from the campus network, so that students cannot accidentally download, or upload things, from the Internet that can-do potential harm. The computers should have virtual machine capability (i.e. via use of a CyberLab server) to run Windows and Linux virtual machines. These VMs can be used to run many open source software that is used to teach cybersecurity students the hands-on learning they desire. Another necessity with the CyberLab is a sufficient budget so that hardware is maintained up-to-date and refreshed within a reasonable time period. Many higher education institutions are now offsetting the cost of the CyberLab with a lab fee on courses that use the lab so that the lab fees 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 what is important is that 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 a budget, then using virtual laboratories with free virtual machines, Like Virtual Box and open source software like Kali Linux or Ubuntu is acceptable (Dampier, 2015).

At XYZ University, there are multiple physical laboratories used for cybersecurity as well as a server used for unlimited virtual machines. The lab will be maintained and run by the department, specifically a professor who will be paid a stipend with a course reduction and is a cybersecurity professional that has the expertise. XYZ University considered using cloud platforms that provide education credits such as Azure, AWS, or Google but not only would the cost not be feasible but the type of software used to teach needs to run in a secure environment that cloud providers could not provide.

Service

At a quality cybersecurity program, a higher education institution will be involved beyond the normal boundaries of the institution and share with others or show how industry theory and practice are incorporated into curriculum. Faculty and curriculum are shared with other schools, to include K-12 schools, community colleges, technical schools, minority colleges/universities to advance cyber defense knowledge. This could mean that faculty speak at other schools or educational conferences and share with them curriculum that is used to teach students cybersecurity.

Quality cybersecurity programs provide students with access to cybersecurity practitioners (e.g., Guest lecturers working in the Cybersecurity industry, government, faculty exchange program with industry and/or government, internship opportunities for students, etc.). This can also be in the form of professional cybersecurity organizations such as ISACA, ISSA or Infragard and for students to network with those members.

At XYZ University, faculty attend and host cybersecurity competitions annually as well as host numerous cybersecurity speakers at no cost to students for 1-day conferences. Faculty also collaborate with other institutions to speak with their students and vice-versa.

Certifications

A cybersecurity degree will only take you so far up the job ladder. At some point in your career, an IT security certification from a reputable third-party organization may be necessary. Certifications make you more attractive to potential employers because they show that you're focused and goal-oriented. If they're not required, they're often preferred, depending on the role. Certifications also keep you marketable in the field as your career progresses, since the threat landscape is constantly changing and businesses—and security professionals—need to keep up.

For this reason, many colleges/universities are building into their cybersecurity program, certification courses. These courses are designed around the material needed to know in order to pass a certification exam. Many companies in today's cybersecurity job market are looking for potential candidates who not only have the cybersecurity education, but the certification to complement the degree. A quality cybersecurity program will offer these courses and even pay for you to sit for the exam.

Cyber security certifications come in all shapes and subjects – from forensics to intrusion to ethical hacking. They are typically administered by independent accrediting organizations like CompTIA, EC Council, ISACA and (ISC)2 as well as vendor specific organizations such as Microsoft or CISCO.

Accrediting organizations often divide their programs into three categories: entry level, intermediate and expert.

- Entry-level certifications are meant to ground you in the basics – foundation principles, best practices, important tools, latest technologies, etc.
- Intermediate and expert-level certifications presume that you have extensive job experience and a detailed grasp of the subject matter.

Therefore, many quality cybersecurity programs develop courses around entry-level certifications that require little or no experience to obtain once the exam has been passed (Author unknown, n.d.).

XYZ University has multiple courses to prepare cybersecurity students for certifications along the way while obtaining their cybersecurity degree. The certifications are some of the most popular and sought after in the market including CompTIA A+, Net+, and Security +, SSCP, CEH, as well as several Microsoft certifications.

CONCLUSION

In conclusion, this article was meant to describe a path to building a successful cybersecurity program, along with specific examples from how one higher education institution, XYZ University, began their journey into building such a program. In order to follow that path, essential components included faculty, courses, credentials, students, Cyberlab, service, and possible certifications. In today's cybersecurity world, many universities are starting cybersecurity programs and in the age where computer labs have disappeared, cybersecurity labs are popping up everywhere. Cybersecurity knowledge, skills, and abilities are important for landing a career in the field and students need to be properly trained. The best way to do that is through hands on learning and teaching inside a cyberlab. The example provided are unique to one university and one cybersecurity professional in higher education, but it mirrors what other universities are doing. In order to educate students in a cybersecurity program, the steps described in the case study are just a guideline but should be highly considered to train students properly.

REFERENCES

Author unknown. (n.d.). *Six Skills You Need to Succeed in Cybersecurity*. Retrieved June 7, 2010 from https://insights.dice.com/cybersecurity-skills/

Author unknown. (2019). *Is attending an NSA CAE IA/CD designated cyber security program important?* Retrieved April 12, 2019 from: https://cybersecuritydegrees.com/faq/nsa-cae-ia-cd-designated-top-cyber-security-schools/

Author unknown. (n.d.). *A guide to cyber security certifications.* Retrieved April 13, 2019 from: https://www.cyberdegrees.org/resources/certifications/

Dampier, D. (2015). *Building a successful cyber-security program.* Retrieved April 13, 2019 from: http://www.dasi.msstate.edu/publications/docs/2015/06/13502Cyber_Security_Workshop_paper_-_Final.pdf

Dickens, B. (2018). *Starting a cyber security program at your school*. Retrieved April 16, 2019 from: https://www.cybintsolutions.com/starting-a-cyber-security-program-at-your-school/

Morgan, S. (2018). *Cybercrime damages $6 trillion by 2021*. Retrieved April 16, 2019 from: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

NSA. (2019). *National Centers of academic excellence.* Retrieved April 12, 2019 from: https://www.nsa.gov/resources/students-educators/centers-academic-excellence/

Online Engineering (2018). *Online Cybersecurity Degree Programs.* Retrieved April 11, 2019 from: https://www.onlineengineeringprograms.com/computer/cybersecurity