Designing cybersecurity curriculum: Exploring the need for industry certifications and experiential learning

Mathew Erickson, Walsh University, merickso1@walsh.edu
Philip Kim, Walsh University, pkim@walsh.edu

Abstract

There is a need to assess the merit and utility of existing cybersecurity curricula. This paper seeks to take a deeper dive into the question of whether a college degree is necessary in the cybersecurity field with an exploration into some examples of US-based undergraduate and graduate cybersecurity degree programs. The authors review the industry standard IT security certifications and governing bodies to compare and contrast the domains and common bodies of knowledge across the various sponsoring organizations. The authors provide their recommendations for building and enhancing undergraduate cybersecurity curricula, in particular new programs should not be siloed within the computer science and information security departments. Faculty should intentionally look to include disciplines outside of the traditional areas of study such as business, psychology, and legal and ethical studies.

Keywords: cybersecurity, curriculum development, certifications, experiential learning, holistic education

Introduction

In light of the global pandemic of 2020-21 much has changed about how universities and colleges recruit, retain, and deliver content to students. Many schools have had to adjust, postpone, and even cancel graduation ceremonies and special events. The push to maintain high quality standards for faculty have increased. In fact, as college entrants have more options for online learning, and no longer feel confined to a local university, administrators have placed an emphasis on differentiation both within and outside of the classroom. Considering this, establishing a high-quality curriculum is of the utmost importance. This requirement is especially important when it comes to cybersecurity. According to Cybersecurity Ventures, “there will be 3.5 million unfilled global cybersecurity jobs in 2021,” with over 300,000 of those jobs in the United States (Morgan, 2020, para. 2).

The unemployment rate in the cybersecurity field has been zero percent since 2011, and Morgan also predicts that 100% of large corporations will have a Chief Information Security Officer (CISO) by 2021, although many of the positions will be unfilled due to lack of experienced candidates (Morgan, 2020). There is a big gap in education for cybersecurity professionals, with many jobs now going to individuals with no college degree, or a liberal arts degree (Morgan, 2020).

As far back as 1998, the criticality of cyber-based systems to national security were recognized. With the release of Presidential Decision Directive (PDD) 63, dated May 22, 1998, President Clinton set in motion a search for the best cybersecurity curriculum to be offered by colleges and universities. PDD 63 stated that
“the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber-attacks on our critical infrastructures, especially our cyber system.” (Clinton, 1998). It also set forth the goal of having achieved and maintained the ability to protect the nation’s critical infrastructures by 2003 (Clinton, 1998). Yet even with this declaration from President Clinton, there is the simple fact that there is still a need for cybersecurity professionals. 17 years later, the day this paper was being written, an article from AP News was published detailing a cyber-attack against the very critical infrastructure that President Clinton was hopeful to protect by 2003. “The hack comprised federal agencies and critical infrastructure in a sophisticated attack that was hard to detect and will be difficult to undo,” (Fox, 2020). The current estimate is that over 40 government agencies, think tanks, IT companies and other non-government agencies were infiltrated (Fox, 2020). Even after two decades of work, there is still a deficient cybersecurity frontline and management group that can step into the roles that can help combat these attacks.

There are a multitude of certification programs available that revolve around cybersecurity, but most of these require a level of understanding that would only be held by someone already working in the field, and therefore do nothing to reduce the gap between high level cybersecurity jobs and education of individuals (Hentea, Dhillon & Dhillon, 2006). This gap will need to be filled, and one of the best ways to fill this gap is with undergraduate and graduate level curriculum that addresses the major needs of the field, as well as appropriate hands-on training in a safe environment. This paper explores both effective undergraduate and graduate level curriculum building, as well as methods of establishing hands on laboratory work that will accelerate student learning, preparing them for the real-world experiences they will face as a cybersecurity expert.

**Literature Review**

**National Centers of Academic Excellence in Cybersecurity**

In 2002, there were 36 schools listed as Centers of Excellence in Information Assurance Education with the National Security Agency, but most of those programs offered only graduate level coursework, and most only offered a single course on Information Security as part of a graduate degree program in computer science or information technology (Logan, 2002). One item that should be noted is that the NSA provided funding to the 36 schools based on the federal guidelines established for being a Center of Excellence in Information Assurance Education. Points were awarded for compliance with these guidelines, with the most points offered for doctoral and graduate programs (Logan, 2002). This is at least part of the reason why most of the schools included in Logan’s research did not include undergraduate courses. Another potential reason is the need for a level of maturity that many schools may feel they will not find in an undergraduate population. Part of the curriculum will inevitably center on hacking methods and hands-on work around hacking, and there may be a concern that these skills could be used for ill purposes in the hands of an immature undergrad (Logan, 2002).

Of the courses offered by the 36 schools, they fell into nine main subject areas:

1. Secure Electronic Commerce
2. Information System Assurance
3. Enterprise Security Management
4. Secure System Administration and Certification
5. Distributed Computing
6. Network Security
7. Computer and Network Forensics
8. Computer Law and Policy
9. Advanced Computer Security

Some of the items that were missing from these schools’ curricula were that few of them offered undergraduate coursework, as well as a lack of specific courses in computer forensics, security policy, security concerns in e-commerce, and legal and ethical courses (Logan, 2002).

In 2020, the program offered by the NSA is now called the National Centers of Academic Excellence in Cybersecurity (CAE), and there are 349 schools that fall into at least one of three categories, Cyber Defense Education (CAE-CDE), Cyber Research (CAE-R), and Cyber Operations (CAE-CO). The CAE-CDE is awarded to schools that provide cybersecurity degrees and/or certificates at the associates, bachelors, or graduate level, the CAE-R is for schools that offer PhD’s and are rated by the Carnegie Foundation Basic Classification system as an R1, R2, or R3, and CAE-CO is awarded to technical higher education programs based on computer science, computer engineering, or electrical engineering programs with hands-on labs and exercises (National Centers of Academic Excellence in Cybersecurity, n.d.).

Certifications or Degrees?

Before discussing the requirements for a degree program, a valid question would be “do businesses need college graduates, or would they be satisfied with work experience and/or certifications?” The answer to this question can be found in a few different places. One is an examination of what professionals are looking for from cybersecurity graduates, and what skills they think are lacking from recent graduates. Another is an examination of the requirements for cybersecurity certifications, and determination of the level of skill required to obtain one, and yet another is a look at how closely undergraduate and graduate degree coursework addresses the requirements that businesses are looking for, and how to enhance the abilities of the graduate to fit those requirements, beyond just the coursework of the degree. However, the starting place for all of these could simply be to check where the businesses are specifically saying what they want: their job postings, which is precisely what was done by Jim Marquardson and Ahmed Elnoshokaty (2020) in their study “Skills, Certifications, or Degrees: What Companies Demand for Entry-level Cybersecurity Jobs.”

In their study, Marquardson and Elnoshokaty (2020) used a web crawler to search for jobs on Dice.com that included key words related to cybersecurity and found 11,938 jobs on June 10, 2019. Once this data was collected and cleaned, they looked for keywords in the job requirements that were related to degrees, certifications, and skills. The results of this showed most job postings (84%) required either an undergraduate degree, or preferred a graduate degree, showing that college education is still preferred by those hiring for cybersecurity jobs.

A little less than one third of the job postings (29%) preferred or required a certification of some type. Of the ones that specified a particular certification, CISSP was mentioned 4.9% of the time, ITIL was mentioned 3.9% of the time, and Security+ was mentioned 2.9% of the time. For skills, the main skills mentioned were Structured Query Language (SQL) in 6.3% of the jobs, “testing” in 5.4% of the jobs, and Excel, Java, Oracle, “consulting”, “database”, and “hardware” all mentioned in between 2-2.6% of the jobs (Marquardson & Elnoshokaty, 2020). This study suggests that based on the data available to the researchers, degrees were much more sought after than industry-specific certifications and technical skills.

Knowing that degree programs are considered relevant to cybersecurity professionals, the next logical question is what do business professionals feel is lacking in the current cohort of graduates. In studies done by St. Clair and Girard (2020), cybersecurity professionals were asked survey questions around working with new graduates in the cybersecurity field. While 73% responded with satisfaction of their interactions
with cybersecurity graduates, many noted that the graduates would have benefited from mentorship or hands-on experience in the way of internships before graduating. Over two-thirds (67%) of professionals felt that recent graduates had satisfactory level of competence, but only 43% felt that the graduates were fully prepared to enter the cybersecurity workplace (St. Clair & Girard, 2020).

Perhaps not surprisingly, many hiring managers feel that some recent graduates lack verbal, writing, and communication skills, which they said is reflected in poorly prepared and presented resumes and CVs. There is also a disconnect between the business professionals that are hiring graduates and the professors that are teaching the graduates on what factors are important in the workplace (St. Clair & Girard, 2020). While business professionals find working with tools and technology important, there was a discrepancy between professionals and faculty. A possible reason for this is that professors are training students that may go into a business with any number of tools at their disposal, depending on the size and budget of the company, and they do not feel they can adequately train to just one platform. One of the things that should be focused on to address this discrepancy is teaching usability and situational cybersecurity as opposed to being focused on one specific vendor over another (St. Clair & Girard, 2020).

While the Marquardson and Elnoshokaty (2020) study show that certifications are only mentioned in 29% of job posting on Dice.com, they are still a relevant part of the cybersecurity training environment. Most certifications require a certain level of work experience, but some (CISA, CISM, and CISSP) allow university degree programs to count towards some or all the work experience requirement (Knapp, Maurer, & Plachkinova, 2017). Some cybersecurity curricula even include the certifications during the degree work. Some universities use the requirements for the CISSP, CISM, CISA, and CEH as the basis for the cybersecurity program, as these are the top four requested certifications by most job postings (Knapp, Maurer, & Plachkinova, 2017). Even for schools that do not teach specifically to the certifications, it is a good idea to use any certification program changes as an opportunity to review the cybersecurity curriculum and ensure that it is staying current.

The CISSP is still considered one of the flagship standards of cybersecurity certification, but it is only available to cybersecurity professionals that have 5 year of experience, making it difficult, if not impossible to acquire without an existing position in cybersecurity. A university degree can be used to count towards one year of the work experience requirement (CISSP Experience Requirements, n.d.). While it will not waive the other four-years of work requirement, the CISSP is still a good starting place for any curriculum, as it covers a broad range of cybersecurity knowledge.

The domains of the CISSP are:
1. Security and Risk Management
2. Asset Security
3. Security Architecture and Engineering
4. Communication and Network Security
5. Identity and Access Management
6. Security Assessment and Testing
7. Security Operations

One way to ensure that the business community is getting the level of graduate that they believe is useful is to build a partnership with local businesses. At Texas A&M University, a partnership was created that ensures not only successful placement of graduates, but continuing education and certification options for local businesses (Nelson & Donham, 2020). This partnership also offers non-degree work at various levels.
of expertise, from cybersecurity technicians, up to cybersecurity managers to ensure a holistic approach to cybersecurity training not only for Texas A&M students, but for the community as whole (Nelson & Donham, 2020).

Discussion

How Should Universities Develop Their Cybersecurity Curriculum?

A cybersecurity degree program should incorporate relevant and up-to-date cybersecurity certifications, provide students with hands on experience, and implement an experiential learning component that allows students to learn and hone their skills in a “real world” setting.

Undergraduate Degree Programs

There are certain prerequisites that must be met before a college or university takes on the task of implementing a cybersecurity degree program. These include faculty interest and the school’s ability to reward and recognize faculty members, textbooks, and a body of knowledge to teach from (including a faculty that possess the knowledge), unsolved problems that can be used for research, administrative and funding support, and finally student interest (Vaughn, Dampier, & Warkentin, 2004). Another consideration when looking at cybersecurity curriculum is the broad umbrella of disciplines it can cover. While it would seem obvious that it lives in Information Technology, it can also be applied to business, political science, psychology, sociology, law, and even agriculture (Hentea, Dhillon & Dhillon, 2006). Regardless of which field or department the student is from, the major consideration for cybersecurity degrees must be centered around preventing cyber-attacks, information security management, and how to make decisions and take actions to control the environment (Hentea, Dhillon & Dhillon, 2006).

There are at least five ways in which a cybersecurity curriculum can be initiated. Existing courses can be enhanced with a cybersecurity component, capstone courses can include cybersecurity components, cybersecurity courses can be created, cybersecurity minors can be created, and cybersecurity degree programs can be created (Whitman & Mattard, 2004). While the easiest of these options would be the first, the current environment dictates the focus be on the last. The focus of this research paper is on creating curriculum for a cybersecurity degree program.

In addition to these curricula considerations, there are also standards set by the National Institute of Standards and Technology (NIST), the National Security Telecommunications and Information Security Committee (NSTISSC) (now known as the Committee on National Security Systems, or CNSS), and the International Organization of Standardization (ISO) that should be used to assist in building a cybersecurity curriculum. ISO 17799 (updated in 2013 to ISO 27002), for instance, was the Information Security education and training standard (Hentea, Dhillon & Dhillon, 2006). The standards set by the NIST and the CNSS are used as guidelines for hiring in government and defense sectors, but the requirements have become the basis for most cybersecurity training and college course work (Hentea, Dhillon & Dhillon, 2006). The issue with this is that while these standards support the roles needed for government and defense, they are not always suited to the private sector.

In 2001, a focus group of industry professionals met to establish the eleven key items that should be minimal criteria for an undergraduate degree in cybersecurity. These items were:

1. Understanding the importance of security for a business
2. Understanding network hardware, network protocols, and computer operating systems
3. Understanding security management
4. Understanding security risk
5. Managing security protection
6. Detecting vulnerability and breaches
7. Responding to security threats and breaches
8. Using communication skills in the workplace
9. Understanding the legal and ethical implications of security
10. Ensuring professional development

The results of the focus group over 20 years ago, remains true today. Employers, hiring managers, and organizations are in need of well-rounded graduates that can address the technical gap, but also the human gap. Cybersecurity graduates need to know how to recognize, understand, and manage risk as well as they need to manage specific security tools.

The career path for a security professional has three steps (entry-level, mid-level, and senior-level security professional), but also needed to include four main components: technical knowledge, technical expertise, business skills, and communication skills (Morneau, 2004). Part of the undergraduate experience should include an understanding of hacking and include both network attacks and network defense as part of the lab experience and include the capstone exercise being a real-world experience (Morneau, 2004).

The main foundations that are required for any cybersecurity graduate will be a strong knowledge of IT infrastructure as a system, rather than the pieces of hardware and software (this will help with issue diagnosis), as well as analytical thinking and problem-solving skills (Sauls & Gudigantala, 2013). These three fundamentals will assist with the application of the other skills the graduate will learn. The ability to think about the infrastructure as a system rather than a collection of parts is essential in security analysis. Lab work and internships help take the practical knowledge and turn it into real-world experience (Sauls & Gudigantala, 2013). Students should also be encouraged to take electives from the disciplines mentioned earlier, as it will help create a broader knowledge and understanding of potential cybersecurity issues.

In creating a cybersecurity undergraduate program at Weber State University, Logan (2002) focused on a few important items, which included technical AND management skills for implementing and managing complex networks, an alliance with the criminal justice department to assist with understanding of forensics, investigation techniques, rules of evidence and law, and looking at all of the components of a complex technology setup, such as security, networks, applications, and desktops (Logan, 2002). The courses included Data Communications, LAN, Computer Crime, Advanced Hardware/Software, and Computer Forensics, as well as Visual Basic and Java programming languages, Systems Analysis, Database Design, and business courses such as Accounting, Business Law, Management, Marketing, Logistics, and Finance (Logan, 2002). Another potential set of courses laid out by Vaughn, Dampier, and Warkentin (2004) include Operating Systems, Database, AI and Expert Systems, Software Engineering, Networks, Computer Security, Computer Forensics, and Network Security, as well as the potential for three different degree tracks with Computer Science, Software Engineering, and Information Systems each having a security focus.

**Recommendations**

Coursework should include real hands-on application and deep instructor-led group discussions of cybersecurity methods, techniques, challenges and difficulties. For example, when students are able to successfully exploit a vulnerability on a virtual machine, this may be the result of a well thought out vulnerability assessment, audit, and attack or it could be the result of an effective script with little to no
thought. Faculty should embed ample time within each module to discuss the process of how the vulnerability was assessed and what alternative methods, tools, and measures could be used help the students become more effective. This also raises the need for another set of coursework that is imperative in a cybersecurity curriculum, and that is Ethics. The groundwork for an Ethics course can be based on the Association of Computing Machinery Code of Ethics and Professional Conduct, which covers various topics, including general ethical principles, professional responsibilities, and professional leadership principles (ACM Code of Ethics and Professional Conduct, n.d.). Certifications are typically only available to those who are already in the security field. One consideration for cybersecurity course curriculum is to include certification trainings and provide the certification as part of the course (Wang, McCoey, & Zou, 2018). This would not only allow graduates to have the skills and training needed to be effective cybersecurity professionals, it would also give them a certification, which has become the holy grail of on the job training and proof of competency.

Wang et al. (2018), from La Salle University in Philadelphia, PA, presented a framework for an Information Security undergraduate degree. In their curriculum design recommendations, there were seven major modules:

1. Overview of Information Security, which covers the “security spectrum” and prepares students for upcoming courses and lab work, as well as the ethical and legal issues involved in cybersecurity and includes a lab with a hardware keylogger to steal information from group partners.
2. Cryptography, which introduces hashing functions, different cryptographic systems and digital signatures, as well as various security algorithms (SHA, RSA, etc.) and includes a lab of the difference between encrypting ECB and CBC image files.
3. File System Security and Access Control, which includes topics on the three components of access control, identification and authorization, access control matrices and licenses, and classification of access control models. This module also includes examination of Linux and Ubuntu file systems and includes a lab on escalating from a regular user to root user and finding the countermeasures.
4. OS Security, which delves into the security issues of various operating systems, including BIOS security, log files, buffer overflows, and common malware and anti-virus tools. The lab for this course covers two items. The first is creating a rainbow table and then using software tools to crack weak passwords, and the second is learning how to apply system built-in tools like Windows Defender and firewalls to harden a host computer.
5. Web Security, which includes topics like HTTP, Web Architecture, Javascript, HTML, cookies, ActiveX and plug-ins, CSS, CSRF, and HTTPS. There are also two labs for this topic. The first involves students learning about session hijacking attacks, and the second is about hardening the browser.
6. Database Security includes topics around SQL injection and DBMS security issues. The lab for this module is a contest between the students to inject SQL statements to bypass authentication on an intranet site setup on the local LAN.
7. Network Security proceeds in a top-down approach through the various layers of network, from Application layer, to Transport Layer, Network Layer, and then Link Layer, and investigates the security concerns at each layer of the network. The lab for this module includes conducting an ARP attack, analyzing the ARP packets generated, and then determining effective countermeasures (Wang et al., 2018).

They also include a module on emerging technologies, which includes discussion of security concerns around IoTs, NoSQL databases, and other technologies that may be coming. This module is meant to serve as an inspiration point for the students’ group projects and is a constantly evolving module as technologies change. The students then begin work on their group projects, which are expected to cover topics that have not been discussed previously. The project is presented by the student group to the class and is written in a lab instruction format for use as hands-on lab problems in later courses (Wang et al., 2018).
Experiential Learning Experiences

A major consideration for any undergraduate or graduate degree in Cybersecurity is a co-op or internship. In 2018, Marc Dupuis from the University of Washington presented a framework used by the school that included a partnership with T-Mobile and used a cohort approach that produced a hybrid of an internship and co-op program that Dupuis called “co-op light” (Dupuis, 2018). This approach could be expanded to include a virtual internship or co-op light structure so that it isn’t restricted to simply a local company. Companies like Apple, Microsoft, and potentially even the US government would be potential prospects for providing these types of opportunities if it means that in return, they will be receiving a more skilled workforce in these areas of cybersecurity.

In 2014, Kumar (2014) introduced a Master of Information Security and Analytics (MISA) degree program at Coastal Carolina University. This course was created due to the increased demand for not only cybersecurity leaders, but also leaders that could use data analysis to enable and improve security. Even graduate programs could benefit from a required experiential learning experience, coop, or internship credit. Graduates of this program would be well suited for a range of careers, including data or security analysts, data or security engineers, data or security architects, department managers or administrators, CISO, or Chief Information Officer. As noted earlier, the position of CISO is expected to be available in 100% of global fortune 500 companies within the next year, but many positions will be unfilled because of lack of qualified candidates (Morgan, 2020). The novelty of Kumar’s program is that it combines the security and analytics elements into one degree, the only one available at the time (Kumar, 2014).

While the program does not result in a certification, it could, as the requirements for the Certified Information Systems Security Professional (CISSP) and the Certified Analytics Professional (CAP) are both included in the coursework (Kumar, 2014). The degree program consists of 10 3-credit courses over a 14-week course length, and includes Cybersecurity, Information Security Policy and Risk Management, Network and Internet Security, Mobile and Web Application Security, Secure Cloud Computing, Data Management and Analytics, Data Mining and Knowledge Discovery, Business Intelligence and Analytics, Data Warehousing and Data Visualization, and Big Data Analytics.

Gaps in Cybersecurity Programs

A potential concern with this coursework is the lack of other non-technical courses. Considering the wide range of challenges, industries, and organizations that deal with information security threats, there is a dearth of inter-department collaboration and cooperation among the various academic disciplines. Even beyond management and organizational behavior courses, cyber security curriculum should seek to address human behavior, consumer behavior, psychology, sociology, legal and ethical considerations. The openness of networks intended to increase open lines of communication, increase collaboration, and provide information transparency are also the same means of attack, ID theft, denial of service attacks. Attackers may have different motivations: money, control, information, hacktivism, political gain, geo-political attacks, etc.

Universities need to consider how to best prepare their students to help their organizations achieve a higher level of security. This takes a multi-faceted approach. Practical hands-on skill, theory, hacking, gray-hat hacking, security certifications, job-training, internships, real-world projects, ethics, verbal and non-verbal communication, psychology, history, analytics, sociology, healthcare, legal and ethical studies, education, social sciences, and even the natural sciences.
As noted previously, the students pursuing a graduate degree will inevitably be the department leaders and CISO’s of the companies they work for. To address this concern, Rick Trilling from Wentworth Institute of Technology created a framework for a Cybersecurity Management program (Trilling, 2018). According to Trilling, as of 2018, 436 colleges and universities offered degree programs in cybersecurity, but a small percentage of those educated managers of the industry. In order to correct this deficit, Trilling offers a combination of cyber technology that falls within the NIST requirements, while also offering a range of business relevant coursework such as accounting, marketing, finance, management, operations, and legal and business ethics (Trilling, 2018).

In addition to this coursework structure, Trilling (2018) also offers a range of possible delivery options, including not only full degree programs, but hybrid programs with cybersecurity focused MBA degrees or other joint discipline degree possibilities. There are some crossover possibilities for management and cybersecurity training, such as legal, risk management, project management, cost-benefit analysis trainings, capital allocation, management control systems, and big data analytics (Trilling, 2018).

**Hands-on Laboratory**

Whitman and Mattord (2004) raised the need for an expansion of hands on laboratory exercises, because “any information security professional worth their salt should be able to view their systems through their enemy’s eyes,” (p.32). As discussed earlier, the ethical challenges of teaching students how to hack systems is real, but so is the need for them to see what is happening from both sides of the table to be able to better defend the attacks when they are in the role. One of the more controversial ways of doing this is by teaching hacking techniques to students. By allowing students to use an attack mindset in the controlled lab environment, they can learn more quickly what hackers are targeting, and therefore work out ways to defend against these attacks more easily than if they were just working on cyber defense techniques (Mink & Freiling, 2006). These types of courses also must have a legal and ethical component assigned to them to ensure that students understand the ramifications of abusing this knowledge.

There are a number of hacking techniques that can be taught in a lab, including but not limited to keylogging, Ubuntu and Unix root escalation, hashing, rainbow table and SAM cracking, OS attacks, session hijacking, web browser attacks, SQL injection, and ARP poisoning (Wang, McCoey, & Zou, 2018). There are also specific methods of attack that can be addressed, such as remote network vs local attack (Yu, 2007). These multiple attack points and methods will allow students to build a wealth of knowledge around how these attacks proceed and will assist them in preparing defenses for these attacks. One of the key components of this type of lab work is the student write-up at the end of the exercise. At a minimum, the student should provide a report on what attacks were attempted, the location or content of any files left on the attacked system, how likely they believe a skilled administrator would have detected their attack, and how they believe the attack could have been prevented (Yu, 2007).

**Conclusion**

There are different strategies to building cybersecurity curriculum, but there are a few items that must be considered when designing one. For any level of program, there must be faculty buy-in, university support, external stakeholder commitment, and an active and productive faculty to stay abreast of changes and advancements within the field cybersecurity. The program should not be siloed within one school (MIS or Computer Science), but should seek to incorporate and work with other departments that can assist in relating the cybersecurity components to areas like cognitive psychology, sociology, health and human services, political science, and legal and ethical studies.
Undergraduate coursework should cover a wide range of areas, from web to operating system to network to file system to database security, and this coursework should be updated at least annually to ensure that it is keeping up with emerging trends and advances in technology. The greater the breadth and relevance of knowledge at the undergraduate level, the great the chance of a student developing useful skills to the business or government sector. In addition, tying coursework into existing certification programs and creating a co-op or internship program is a great way to provide additional value, not only to the student but to the hiring company after graduation.

Well known industry certifications, common bodies of knowledge, subject domains should be included within any cybersecurity degree program as these are the standard bearers for the external stakeholder community as well as minimum requirements for entry-level job postings. Additionally, cyber security programs should seek to incorporate experiential learning environments, such as instituting a hands-on laboratory, internships, coops, and allowing students to work on real world problems. This will reinforce students learning outcomes and provide opportunities to demonstrate the mastery of course concepts. While there are arguments for and against teaching actual hacking methodologies and practices, there is a growing acceptance of utilizing gray hat hacking techniques to better understand malicious attack strategies.

References


