SAIS 2022 Proceedings

Southern (SAIS)

4-1-2022

Effectiveness of Bridging Master Program in Cybersecurity and Industry in US: Program Comparison and Analysis

Shalaka Kulal
Kennesaw State University, skulal@students.kennesaw.edu

Xin Tian
Kenensaw State University, xtian2@kennesaw.edu

Zhigang Li
Kennesaw State University, zli8@kennesaw.edu

EFFECTIVENESS OF BRIDGING MASTER'S PROGRAM IN CYBERSECURITY AND INDUSTRY IN THE US: PROGRAM COMPARISON AND ANALYSIS

Shalaka Kulal
Kennesaw State University
skulal@students.kennesaw.edu

Xin Tian
Kennesaw State University
xtian2@kennesaw.edu

Zhigang Li
Kennesaw State University
zli8@kennesaw.edu

ABSTRACT

This paper investigates the existing curriculum of cybersecurity programs the U.S. universities and provide suggestions to improve the programs to fill the gap between academia and industry. In the current state of science and technology, the need for strengthening cyber security has been growing in every developed country and transforming it into one of the most critical sectors of society. In this research, we have shown the essential role of cybersecurity professionals in preventing, detecting, responding to, and mitigating cyber-attacks using a case study of a targeted cyber-attack of a large organization. We presented a threat-centric framework for developing cybersecurity competencies and detailing the steps involved in building a cybersecurity master's program. Consequently, we have made some suggestions regarding a holistic approach to address these issues. This paper is intended to fill the gap of careers and research in cybersecurity and related areas.

Keywords

Cybersecurity, Education, Curriculum

INTRODUCTION

In the recent past, cyber-crime activities have been on the rise globally. This has led to a growing concern by institutions, individuals, and the international community to develop and design system technology to protect networks and to ensure the security of their sensitive data. As a matter of fact, cyber-crime is not a new phenomenon. Many citizens in the U.S. and other countries worldwide consider cyber-attacks as a major threat to their personal data. Lots of organizations have suffered both internal and external attacks. As a result, the demand for skilled personnel who graduated from cybersecurity master's programs continues to be high, as government agencies and companies face ongoing threats like data breaches and hacking. Furthermore, graduates can anticipate a strong job market. A master's in cybersecurity is a good choice for people looking to obtain the technical proficiency to manage and detect threats to valuable and sensitive data, computer, and networks systems.

Even as measures are put in place to curb the ever-increasing threats, the role of the education system, more so, the cybersecurity curriculum, has been put in the spotlight. Accurate and relevant areas covered by the cybersecurity courses and vital skills can never be underestimated in combating these criminal attacks. This paper seeks to unravel the similarities and differences of master's degrees in cybersecurity offered in 10 different universities with a focus on their curriculum. The findings are from the top 10 universities offering cybersecurity master's degrees in the U.S. They are Florida Institute of Technology, Melbourne, FL; New York University, New York, NY; Boston University, Boston, MA; Webster University School of Education, MO; Kennesaw State University, Kennesaw, GA; University of Southern California, Los Angeles, CA; Maryville University of Saint Louis, St. Louis, MO; The George Washington University, Washington, DC; John Hopkins University, Baltimore, MD; University of Virginia, Charlottesville, VA. This paper is organized as below. Following by literature review section, we compared the curriculum among the Mater's programs in cybersecurity from these ten universities. And then we analyzed the job descriptions from 30 typical companies and then gave some suggestions to bridge the program and industry.

LITERATURE REVIEW

Cybersecurity in higher education

Given the situation about the threats and cybercrimes happening around the world, it is obvious that there should be improvements regarding cybersecurity in current and future IT professionals. The cybersecurity field is related to the defense industry, and hence most of the cybersecurity programs are heavily influenced by the government or the defense industry agents (Mogoane & Kabanda, 2019). The cybersecurity education programs should be related to more than one branch of Information Security. This will improve efficiency, readiness and develop the cybersecurity education process (Rahman et al., 2020). Human nature mistakes, malicious activities, and immoral behavior continuously pose threats to IT systems. With the advent of information and cyber security, and with the lack of qualified professionals, tackling this problem is more important than ever before. Professional shortages, while they are a widespread phenomenon, are more distressing for emerging nations, which also must deal with other contextual challenges like inadequate resources for content and digital security, poor security hygiene, and piracy (Cheung et al., 2011).

There are currently 1 million unfilled cybersecurity jobs worldwide, according to Cisco (Callen & James, 2020). Demand in the cyber security job market is highly lucrative, while supply is lagging. Jobs posted in the U.S. alone have increased 74% in five years, with 209,000 jobs available, according to Forbes (Callen & James, 2020). Standard cyber security positions are in short supply because there aren't enough talented and qualified candidates. The cybersecurity field is highly sought after, with engineers so far ranking amongst the highest. "The need for seasoned cybersecurity engineers who can detect and neutralize threats is making it hard to retain them," the Wall Street Journal noted (Boulton & Norton, 2015). A substantial amount of academia has been launching cybersecurity engineering programs because demand for cybersecurity engineers is so strong and qualified professionals are in short supply. As a result, salaries, job outlook, and job opportunities are favorable. A rapidly changing world global market makes certain that cybersecurity graduates have the ability to compete. A cybersecurity student must not only possess advanced sciences and technologies, but also have the knowledge, skills, and abilities needed to advance in the field to contribute and progress in this highly lucrative and demanding field (Mouheb et al., 2019).

CYBERSECURITY CURRICULUM

As cyber-attacks attacks are becoming more widespread, cybersecurity education is becoming more and more important. Several cybersecurity curriculums have been proposed in this context. The current literature on cybersecurity curriculum design approaches is reviewed and analyzed in this section.

Florida Tech provides an interdisciplinary program for information assurance with cybersecurity that, through its degree curriculum, focuses on the various threats cybersecurity professionals not only face today but will also face in the future. At Boston University, the Master of Science in Cybersecurity is part of the Computer Science department. Students pursuing this MS certification in cyber security must complete the same 8 graduate courses and 32 credits as those seeking the MS in Computer Science. Master's candidates are required to complete five courses from the breadth (core) list. Webster University's BS in Computer Science with an emphasis in Cybersecurity (BS/CYB) program offers an educational experience designed to develop the necessary background to perform as analysts, administrators, and managers for cybersecurity offices within government and industry. This program requires 36 credit hours of coursework with 21 credits for core courses and 15 credits for electives. The hallmark of the program is that it is structured around specific skill sets rather than the traditional subject matter approach used in many cybersecurity programs. Another key component of the program is its hands-on learning environment. This university offers MA in National Security Studies / MS in Cybersecurity program with 54 credit hours. One can get to know about the stupendous offerings of this university by availing one of the details by browsing through the site. The cybersecurity master's program at The University of Arizona is fully online with 33 credits required. As for The University of Southern California, the master's program is fully online with a total of 28 credits required. The curriculum fosters an understanding of how to develop a security policy and how policy drives technology decisions. The Maryville University of Saint Louis provides bachelor's as well as fully online master's degrees in cybersecurity where students get hands-on experience in their virtual lab, the Cyber Fusion Center, where they take on real-world cyber security challenges. The Master of Engineering in Cybersecurity Analytics at The George Washington University, Washington, DC is a fully online program that blends the technical, managerial, and soft skills needed to manage security analytics in a complex environment. The program combines a comprehensive curriculum covering traditional methods for intrusion detection and risk assessments with a new emphasis on analytics in big data, semantic analysis of open-source intelligence, and privacy protection. John Hopkins University offers a fully online Master of Science degree in Cybersecurity with 4 concentrations to choose from: Analysis, Assured Anatomy, Networks, and Systems. Table 1 shows the comparison and categories of these cybersecurity programs.

CYBERSECURITY PROGRAMS - SIMILARITIES IN CURRICULUM OF THESE UNIVERSITIES

A career for Cyber Security Master's Degree Programs professional from all the ten universities awaits people who effectively complete programs. Some get jobs from government organizations or single large corporations. Others work with network security companies, which deal with the needs of several contracts at a time. Graduates fill different roles as security architects, vulnerability analysts, network penetration testers, and security analysts. In most universities, the master's degree in cybersecurity is designed for about 30-45 credit hours offered on campus or online. But looking at the current trend, most universities, for example, the University of San Diego, offer their courses entirely online. The courses administered in most of these universities are through online voice-over materials, which on most occasions are supplemented with reading materials, recorded voice notes, and exams. Due to the varying credit requirements at different universities, it can take about 1-3 years for a student to obtain his or her master's degree.

Master's degree in cybersecurity curriculum must always contain courses that have a direct relation to cybersecurity, but then depending on the student specialization and interest, this may vary. A student may opt to be a generalist in the field, that is, only undertaking courses that revolve around cybersecurity, but in cases where the student specializes, they will mostly undertake courses that revolve around their area of specialization. The student who intends to specialize in an area of interest in any of the 10 universities has the following common areas to specialize in, this includes but is not limited to computer forensic(s), information assurance, and system security. Whereas the 10 universities offer different courses on cybersecurity, there are common core courses offered in all the universities. The fundamental courses include cyber law and ethics, which deal with the legal aspect of a business. Another common course is computer security, which explores more on computer systems and their functions, and lastly, a course on network defense which deals with network security. However, the content of the courses varies from school to school.

For one to be admitted as a student in any of the 10 universities to pursue a master's degree in cyber security, he or she must have a strong academic background in the areas of computer science or information technology. However, prospective students with 2-3 years of experience in cybersecurity areas are also considered. Furthermore, some universities like DePaul University offer pre-requisite courses before admitting you for a master's degree with a minimum GPA range between 2.4-3.0.

In all the ten universities, for one to get enrolled on a cybersecurity master's degree, he or she must have undertaken undergraduate degree programs such as those of engineering or computer science. Most of these universities prefer those students who have excelled well in their previous studies. While at the college, the student must undertake classwork and come up with a project. In most cases, the classwork accounts for up to one year while the project lasts for one year. When developing a project, students are encouraged to come up with a thesis which they are supposed to defend on a panel of the committee. This shows the competency of the student before being awarded a master's degree.

In most of these universities, students must learn programs that are needed to design network systems so that once in the field, they can help government, corporate and other institutions to identify and mitigate security risks. Students are taught how to identify theft, piracy, infrastructure vulnerabilities, and proprietary information. Besides, most of these universities offer room for those students who wish to conduct doctorial level research in cybersecurity. Most of these universities encourage students to apply for scholarships in the cybersecurity master's degree. This means some students end up paying nothing for the whole program while others will pay full. Besides, others might cost-share school fees with the college, relieving them the burden of school fees. Many of these universities have been recognized as international institutions. They not only accommodate students from the US but also different parts of the world. Most of the foreign students originate from developing countries such as Africa and Asia.

Some of these universities offer both traditional degree programs and professional development programs in cybersecurity. This is evident in George Washington University and Maryland University. In George Washington University, their master's degree is administered through the college of professional studies, in which students must undertake 60 credit hours in certain courses. Most of the intakes carried out in these universities occur during the fall of spring and summer semesters. A student may either be taken as full or part-time for a period not lasting for more than three years. Once students are admitted, they can either opt to take their courses online or pay a visit to the classroom. Most of these universities prefer students attending classrooms since cybersecurity courses are very critical, and students need not miss important concepts to hasten understanding.

Some of these universities employ those programs that may require students to play the CSO or CISO role. Besides, other programs require students to gain more experience working in IT. Most of these colleges train students in cryptography, application security, and network security.

DISCUSSION

Media coverage of cybersecurity has recently increased; for almost two decades, the topic has been discussed seriously by the government, industry, and academia. It should be noted that there are some differences between authors in their definitions and interpretations of cybersecurity. Many experts submit that the topic is over-hyped and artificially inflated due to fearmongering and the use of terms such as cyber-warfare that are meant to trigger an emotional reaction rather than a rational one. Most of the curriculum shows that the most used language for cybersecurity education is python. In the cybersecurity field, Python has become the go-to programming language for those with a limited background in programming, as it has a generally short learning curve. Any security professional with a basic understanding of Python can begin coding and implementing their code quickly once they understand its basic syntax. Due to Python's massive library, penetration testers and cybersecurity analysts no longer need to reinvent the wheel when performing routine tasks. Also helping cybersecurity professionals is that Python is easy to code, so they can develop solutions with little time, and with rather simplistic code.

We researched different cybersecurity skills and tools required for a cybersecurity job in 30 companies and found Azure cloud services are the most required skills for a cybersecurity job. Hence, we can include Azure cloud services in our cybersecurity curriculums along with the CISSP and GISCP Certifications. Also, Splunk and Linux are the common requirements for cybersecurity jobs. These results are limited to 30 US companies.

SUGGESTIONS

There has been a general lag in education between what is done in the field and what is taught in school. Changing the lab environment to reflect recent events, which have made the news, will be necessary for this to be useful (Kim & Beuran, 2018). A cybersecurity educational program can be made more effective with the suggestions given in this section.

Involving their inaugural cohort of college students in a variety of projects throughout the initial semesters of their master's and Ph.D. programs, a highly certified cybersecurity graduate faculty will function as a center for the exploration and dissemination of fresh cybersecurity analysis, standards, and codes of performance (Rowe et al., 2011). This can foster postgraduate labor to support the nation's cybersecurity needs. For maximum results, cybersecurity scholars should engage in interdisciplinary applied sciences. We advocate that universities spin-off cybersecurity into a specialized program that covers not solely network safety and database expertise, but also stability and safety controls in addition to real-world protection services (Callen & James, 2020). The M.S. and Ph.D. applicants in cybersecurity engineering are required to gain abilities to layout, engineer, and verify the software program, hardware, and applications that contain our information and communications infrastructures. These abilities are regarded as a core part of a cyber shock commando's skillset for current and long-term eventuality response purposes.

The world community was impacted when it became aware of massive ransomware attacks against entities such as the National Health Service (NHS) and dozens of large companies in more than 150 countries. WannaCry involved a strain of ransomware called "WannaCry" that relied upon a flaw in older versions of Microsoft Windows that was stolen from the NSA and then released to the world by a hacker group called "Shadow Brokers". Cybersecurity cannot be considered an afterthought when designing and developing new technologies. The laboratories should also include networked systems of tens, hundreds, or even thousands of nodes to simulate realistic real-world environments. Integrating physical environments with software and hardware, cyber ranges provide students with the opportunity to select various attack targets online and analyze their responses. Students can then use what they've learned in both traditional cybersecurity courses and more practical application courses. There are numerous approaches that can be pursued to close the severe cybersecurity skills gap between supply and demand. One way is to develop industry-university partnerships to develop more effective cybersecurity graduate programs. Current academic programs are unable to satisfy market demand, so the industry should subsidize the cost of developing new programs to close the skills gap. This will also help ensure that students are prepared for the future workplace. Because of the advanced skill levels required, there are several prerequisites encouraging national standards, including an understanding of standards development, security concepts, and hands-on skills using prevalent security tools. It's important that professional certifications reflect real knowledge based on real experience.

CONCLUSION

This conclusion is limited to research in 30 US companies and 10 US universities that provide cybersecurity master's and bachelor's degrees. When we check the most required skills for a cybersecurity job it shows cloud services, different certifications, Python and Java languages, and risk assessments (Shown in Figure 1). U.S. universities can include these skills in their curriculum to improve the recruitment of students. Kennesaw State, Maryville, and George Washington Universities do include cloud certifications, which gives students the opportunity to stand in the job field. In some companies it is required to have cybersecurity Degree which most of the universities doesn't offers. Universities with cybersecurity programs including these skills in their curriculums can help students build their future in cybersecurity.

Table 1. Cybersecurity Program Comparison and Categories

University Name	**Management & Law**	**Cloud Computing**	**Networking**	**Data Related**	**Cryptography**	**Research Opportunity**
Florida Institute of Technology, Melbourne, FL	Biometric technology and the privacy and legal issues surrounding it	NA	NA	Data mining and machine learning methods in cybersecurity scenarios	Communications encryption	Yes
New York University, New York, NY	Introduction to US Law And Cybersecurity Governance and Policies	NA	Computer Networking	NA	NA	NA
Boston University, Boston, MA	NA	NA	Network security	Data and information security	Cryptographic methods	Yes
Webster University School of Education, MO	NA	NA	NA	NA	Encryption Methods and Techniques	Practical Research in Cybersecurity
Kennesaw State University, Kennesaw, GA	Management of Cybersecurity	Cloud Security	Networking	Data Communications	NA	Capstone in Cybersecurity Management
University of Southern California, Los Angeles, CA	Key management	NA	Secure networking	NA	Use of cryptography	Yes
Maryville University of Saint Louis, St. Louis, MO	Knowledge of vital business concepts	Cloud Certified Security Practitioner	NA	NA	Certified Encryption Specialist	Yes
The George Washington University, Washington, DC	NA	Cloud computing security	Network defense	Applied data analytics and Security data visualization	NA	Yes
John Hopkins University, Baltimore, MD	NA	NA	Networking	Data Analysis	NA	Yes
University of Virginia, Charlottesville, VA	Cybersecurity Policy, Law & Ethics	NA	NA	Data Analytics	NA	Yes

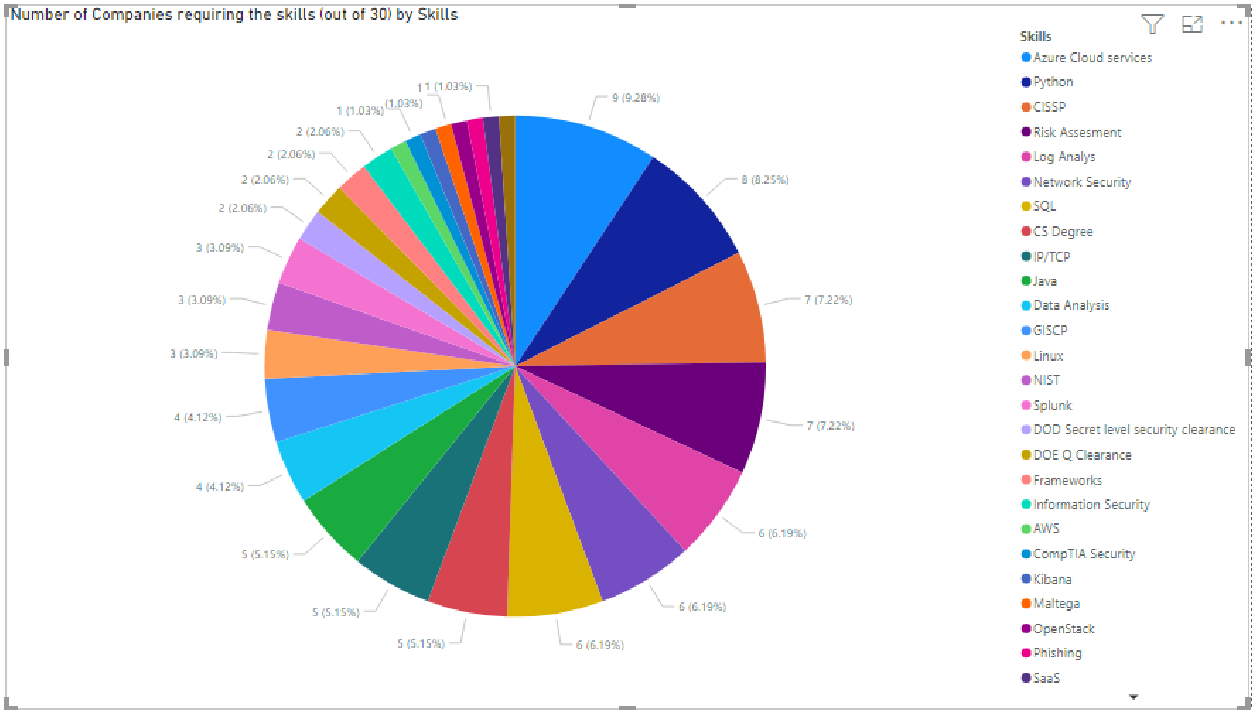

Figure 1. Cybersecurity Job Skills

REFERENCES

1. Boulton, C., & Norton, S. (2015). Pay for Mid-Level Cybersecurity Talent Is Soaring. *The Wall Street Journal*. https://www.wsj.com/articles/BL-CIOB-6166
2. Callen, J., & James, J. E. (2020). Cybersecurity engineering: The growing need. *Issues In Information Systems*, *21*(4), 275–284. https://doi.org/10.48009/4_iis_2020_275-284
3. Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011). *Challenge Based Learning in Cybersecurity Education*. 6.
4. Kim, E., & Beuran, R. (2018). On designing a cybersecurity educational program for higher education. *Proceedings of the 10th International Conference on Education Technology and Computers - ICETC '18*, 195–200. https://doi.org/10.1145/3290511.3290524
5. Mogoane, S. N., & Kabanda, S. (2019). *Challenges in Information and Cybersecurity program offering at Higher Education Institutions*. 202–190. https://doi.org/10.29007/nptx
6. Mouheb, D., Abbas, S., & Merabti, M. (2019). Cybersecurity Curriculum Design: A Survey. In Z. Pan, A. D. Cheok, W. Müller, M. Zhang, A. El Rhalibi, & K. Kifayat (Eds.), *Transactions on Edutainment XV* (Vol. 11345, pp. 93–107). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-59351-6_9
7. Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology*, *10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393
8. Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011). The role of cyber-security in information technology education. *Proceedings of the 2011 Conference on Information Technology Education - SIGITE '11*, 113. https://doi.org/10.1145/2047594.2047628