Meeting the Demand: Building a Cybersecurity Degree Program With Limited Resources

Scott Bell
School of Computer Science
and Information Systems
Northwest Missouri State University
Maryville, MO 64468
Email: sbell@nwmissouri.edu

Michael Oudshoorn
School of Engineering and Computer Science
High Point University
High Point, NC 27262
Email: moudshoo@highpoint.edu

***Abstract*—This innovative practice paper considers the heightening awareness of the need for cybersecurity programs in light of several well publicized cyber-attacks in recent years. An examination of the academic job market reveals that a significant number of institutions are looking to hire new faculty in the area of cybersecurity. Additionally, a growing number of universities are starting to offer courses, certifications and degrees in cybersecurity. Other recent activity includes the development of a model cybersecurity curriculum and the creation of a program accreditation criteria for cybersecurity through ABET.**

This sudden and significant growth in demand for cybersecurity expertise has some similarities to the significant demand for networking faculty that Computer Science programs experienced in the late 1980s as a result of the rise of the Internet. This paper examines the resources necessary to respond to the demand for cybersecurity courses and programs and draws some parallels and distinctions to the demand for networking faculty over 25 years ago.

Faculty and administration are faced with a plethora of questions to answer as they approach this problem: What degree and courses to offer, what certifications to consider, which curriculum to incorporate and how to deliver the material (online, face-to-face, or something in-between)? However, the most pressing question in today's fiscal climate in higher education is: what resources will it take to deliver a cybersecurity program?

I. Introduction

The history of hacking is older than today's networking systems, so there should be little surprise that the Internet has become the target of a rapidly growing number of attacks. A brief look at a few of the earliest attacks [1] shows that they have essentially always existed on the Internet.

1969 Arpanet Launched
1971 John Draper (Cap'n Crunch) hacks phone system with toy whistle,
1983 Internet founded by splitting Arpanet into military and civilian networks,
1983 Kevin Poulsen arrested for breaking into Arpanet,
1984 Fred Cohen develops first PC virus,
1984 Bill Landreth convicted of hacking into NASA and DoD computer systems,
1986 the "Hacker's Manifesto" published by Loyd Blankenship [2], and
1988 the Morris worm spread itself across the Internet.

The gradual increase in both the quantity and voracity of attacks during the early years of the Internet should have alerted companies to the growing threats involved when moving business to this medium. The lack of an adequate response has produced a target-rich environment for attackers, and an Internet-based world that is scrambling to catch up. A few examples of more recent attacks show just how serious the problem has become [3]:

- Equifax breach: 145.5 million accounts compromised (2017),
- Uber breach: 57 million records compromised (2016), and
- Yahoo breach: 3 billion accounts compromised (2016).

In addition to data breeches resulting in the theft of personal information, other attacks such as worms and viruses are exceptionally disruptive and cause substantial loss of productivity. For example, the recent WannaCry ransomeware (2017) attacked over 200,000 systems in 150 countries, including numerous hospitals [4], potentially putting patient lives at risk and displaying just how vulnerable we all might be.

Lloyd's of London, the British insurance company, estimates that the world-wide economic losses due to cyber-crime rose to as much as $450 Billion in their 2017 Counting the Cost Report [5]. The Ponemon Institute's report on the cost of data breeches [6] estimates a single data breach costs the average company about $3.62 million. In a separate study, Juniper Research Group estimates the annual cost of data breaches worldwide could reach $2.1 trillion by 2019 [7], [8].

Every year, the quantity and size of cyber-attacks, the volume of data compromised, and the cost of managing a breech seems to eclipse that of the previous year. One primary factor is the rapid growth of the Internet infrastructure and its usage over the past two decades combined with a relative lack of growth in the number of individuals with the necessary skills and knowledge to defend digital assets. Until recently, and still in many organizations, system security positions and equipment are often considered to be overhead expenses, and not looked at as insurance or protective investments. As such, industry has been reluctant to adequately invest in protection for their network and digital resources.

Universities and other educational institutions have, for the most part, followed the lead of industry, leaving the

978-1-5386-1174-6/18/$31.00 ©2018 IEEE

development of security professionals to technical institutions, community colleges and training programs. However, several factors are leading to a change in this philosophy: *a*) the increase in public attention towards cybersecurity, *b*) the resultant increase in interest from students seeking a cybersecurity related qualification, *c*) pressure from the profession through the Cyber Education Project [9], *d*) the expectation of the computing community that cybersecurity be addressed in several topics within the curriculum [10], and *e*) the recent cybersecurity curriculum guidelines [11] and accreditation criteria [12], [13] have captured the attention of academic institutions. Many are now considering the development of cybersecurity related courses or programs to address this demand.

II. Considerations

A. Faculty Demand

The current situation shares some similarities with the rush to add networking courses and faculty in the 1980s as a result of the birth, and proliferation, of the Internet. At that time many universities struggled to find suitably qualified faculty to teach newly introduced networking courses. Furthermore, the resources available to support these courses were limited to textbooks as it was rare to find substantial course material over the then fledgling Internet. The pressure to find faculty with expertise in networking drove salaries up for faculty in that field. In the 1980s the push was to insert a course or two on networks into the curriculum and potentially consider developing distributed systems courses as a related topic area.

Similar to the networking proliferation of the 1980s, the number of vacancies advertised in cybersecurity related faculty positions [14] is driving salaries upwards for those with appropriate expertise. Currently in the US, a visual inspection of the advertised academic jobs in computer science in any given week shows that $\frac{1}{4}$ to $\frac{1}{2}$ of the vacancies mention cybersecurity as a desired area of expertise. The demand for cyber-expertise is high, both within academia and industry, and the supply of individuals with the necessary qualifications is relatively low. While the expectation is that supply will meet demand over time as new programs are developed, and more Ph.D.'s in cybersecurity are produced, it will not occur overnight.

The crisis in networking faculty was related to the need to introduce one or two courses into the curriculum. Similarly, the cybersecurity faculty demand is driven by the need to add a cybersecurity element into every existing accredited program as a result of changes in the curriculum guidelines [10], [11] and the accreditation requirements [12], [13]. This is compounded by the push for complete programs in cybersecurity, rather than one or two courses, to address the sudden demand within the field.

In contrast, the networking demand appeared suddenly as the Internet phenomenon spread globally, whereas the need for cybersecurity has been omnipresent, albeit largely ignored. It has been the recent spectacular failures of cybersecurity through data breeches, and the associated publicity, coupled with high salaries in the profession and the prediction of continued strong job growth for information security analysts (28% growth in job outlook through 2026) [15] that has, at least in part, generated the demand for cybersecurity programs. Even with a number of institutions moving to introduce cybersecurity programs, it is predicted that over a million positions will remain unfilled by 2021 [16], [17], and that the cybersecurity market will grow from $75 billion in 2015 to $170 billion by 2020 [16].

B. Program Outcome Demands

Another interesting contrast is the diversity of the necessary skill sets. Employers are looking for a wide variety of skills and educational backgrounds to address the need for cybersecurity professionals. Some positions require deep knowledge of tools and techniques to identify and neutralize threats, or to scan the environment regularly for such threats to prevent them from occurring. Some positions are policy-centric and revolve around identifying and deploying best practices to prevent and manage cyber risks. Others are more technical and require the development of resilient software, or the development of new cryptographic algorithms. As the skill set varies, so too does the selection of educational pathways to support the vast array of jobs opening up within this diverse field.

Universities are traditionally focused on 4-year degrees and are interested in providing breadth of knowledge to graduates. Certification programs tend to be much shorter in duration and highly focused on a more narrow knowledge area or skill set. As a result of the strong demand for cybersecurity professionals across a wide array of jobs, there is demand from employers for graduates of all kinds of programs.

C. External Resources

For institutions looking to deliver cybersecurity degrees, there is a wealth of resources available ranging from certification courses, Centers of Excellence, online textbooks and teaching resources, to colleagues who have already developed and are offering cybersecurity degrees. There are several programs that could be used as models for any new program, including programs at both the graduate and the undergraduate level. Programs vary from those focused on policy matters, and others focused on deeply technical skills, through to programs that offer minors in cybersecurity, or only a subject or two related to cybersecurity embedded within a computer science or information systems degree.

Any new program merely needs to identify what area it wants to emphasize in order to identify a number of exemplar programs that could serve as a model starting point. Furthermore, the emerging model curriculum guidelines for computer science [10], information technology [18], [19] and cybersecurity [9], [11] provide clear direction to new programs in terms of what is necessary within a program in order to produce graduates that industry would find sufficiently broad while possibly still having some measure of specialization within cybersecurity. While it is clear that universities cannot fully address the shortfall in the workforce of cybersecurity

professionals, there is an opportunity for new programs to develop their own unique focus and strengths to meet this still-growing demand for well-prepared cybersecurity professionals.

D. Divergence from the Networking Model

When considering cybersecurity as a field of academic study, it begins to diverge in comparison to the networking programs mentioned previously. While the scope of computer networking has expanded over the last 20 years, the core knowledge has remained relatively consistent. The volume of work for network administrators has grown and become more complex. However, the boundaries are well defined, and training for these jobs has been outlined well at this point. There are specializations that stack upon basic certifications or academic training, but for the most part, the components and tasks can be contained within that one pathway.

Given the wide variety of environments, activities, and demands that exist within today's Internet, cybersecurity tasks have grown across several disciplines. There is the information technology aspect, which involves the day to day management of network security components such as hardware, software, users and data. Then, there is the computer science side, where individuals learn to incorporate best practices and technology into system designs and software development. There is also the management perspective, which includes risk assessment, data analysis, and the decision-making processes which are based on organizational goals, and not necessarily based solely on security and technical merits. While there are many common academic components within each of these disciplines, the overall skill sets for each are dramatically different and require a rather diverse set of courses to meet the needs of each job description. This makes it difficult (and more likely impossible) for a single degree program or curriculum design to cover the entire breadth of material embodied beneath the current umbrella of cybersecurity. This is especially true when consideration is also given to other academic demands at a small university. This can be seen in the various curriculum standards presented within each discipline.

III. The Path Towards a Security Program

Northwest Missouri State University is a moderate sized, regional, university and offers bachelor degrees in Computer Science, Digital Media, and Management Information Systems. In 2002, a single course in computer networking was offered and became a required course for students enrolled in both the Computer Science and Digital Media degree programs. Two years later, a minor in Networking was added and by 2007, this program included the option for students to prepare for CISCO certifications. A set of five courses were developed and an isolated lab was built to support the certification program.

For a brief time, the program flourished, with numerous students pursuing the minor and successfully finding jobs. The decline in computer science enrollment in the early 2000s, and a reduction in student interest, led to course enrollment levels which became untenable. As a result, by 2010, the advanced networking courses were no longer being offered and by 2014, the minor, while still on the books, was no longer available to students.

Meanwhile, a course in Network Security was developed as a required component for an Applied Computer Science graduate program and was cross-listed as an elective for undergraduate Computer Science students. Interest in the subject from undergraduate students escalated over the course of several years. In response to this growing interest, as well as recommendations from a professional advisory team, an emphasis area in Information Assurance and Security consisting of 3 courses was created in 2015 for students majoring in Computer Science.

Over the past two years, strong student interest in the emphasis area, growing interest from prospective students and positive feedback from the professional advisory team led the School to create a new undergraduate program in cybersecurity, set to launch in the Fall 2018 semester. Several students, both current and prospective, are already committed to enroll in the program once it is available.

IV. Taking The Leap Into Cybersecurity

A. Motivation

Over summer of 2017, the decision was made to seek approval from the Missouri Department of Higher Education to offer a Bachelor of Science degree in cybersecurity. A group of six interested faculty were identified and charged with developing the curriculum for a cybersecurity degree and completing all the necessary paperwork for internal approvals (School of Computer Science and Information Systems, Faculty Senate, Board of Trustees, and several other internal committees) and approval by the Missouri Department of Higher Education.

The motivation for developing the new degree was driven by a number of factors:

1) Demand: there was interest in a cybersecurity degree exhibited by existing students through the cyber-defense club, and through inquiries made by prospective students.
2) Enrollment numbers: there had been a sharp and sudden decline in the number of international students enrolled in the Master of Applied Computer Science degree and there was pressure to identify alternative programs to attract students.
3) Income: the State of Missouri is cutting funding to higher education and additional revenue streams are necessary to offset the reduction in state funding.
4) Industry: interest in a cybersecurity program through the professional advisory team as a result of recent publicity surrounding cybersecurity breeches, and the need for competent and well-trained cybersecurity professionals in industry.
5) Employment opportunities: job growth projections as made by the Department of Labor [15] and others.

These factors, together with an interest from the faculty, and the pre-existing networking/network security lab which could

serve as a basis for a cybersecurity lab, drove the development of the cybersecurity program.

B. Program Focus

Once a decision was made to offer a cybersecurity degree, the priority was to determine what focus the degree would have. The cybersecurity model curriculum [11] identifies eight knowledge areas within cybersecurity, any one of which could become a focus of the degree. The eight knowledge areas are:

1) data security,
2) software security,
3) component security,
4) connection security,
5) system security,
6) human security,
7) organizational security, and
8) societal security.

While it is important to cover each of these areas, there is no need to draw on each equally. Examining the existing courses in Computer Science offered at Northwest Missouri State University, it was decided that a focus on data security (via the database course), software security (via the programming classes), connection security (via the networking classes, and system security (via the system administration course) would serve as the backbone of the program. These courses already existed and would require some modification to be suitable to both computer science and cybersecurity programs, but adapting them would minimize course proliferation as no additional faculty were being hired to support the new program. This also benefits the computer science program as the 2013 computer science curriculum guidelines [10] suggested cybersecurity ought to be covered inside all computer science programs. This was not occurring to the extent desired at Northwest Missouri State University and this strategy also allowed that matter to be addressed.

Program outcomes for the cybersecurity program were adopted from the emerging ABET cybersecurity accreditation criteria [13]. This was done to ensure the outcomes were consistent and aligned with industry expectations and left the door open for future accreditation if that becomes a school goal. The computer science program had previously adopted outcomes modeled in part on the ABET Computer Science Program criteria [12] and hence this decision aligned with previous decisions regarding program outcomes.

Once program outcomes were determined, the question of delivery mode was addressed. Northwest Missouri State University's School of Computer Science and Information Systems has long used traditional face-to-face delivery methods with a strong emphasis towards hands-on practical experience. For the faculty, this was the most comfortable approach. Students at Northwest Missouri State University are typically resident students and hence this delivery mechanism suits these students. However, with recent cuts to Higher Education in the State of Missouri, there has been increasing pressure to deliver programs online or in remote locations, such as Kansas City, where there is a larger population base. The pressure from administration to teach the cybersecurity program online remains, but the decision was made by the faculty to only offer the program in face-to-face mode until such time as all courses were developed and there was suitable experience with the program inside the School.

C. Industry Support and Input

After the curriculum was identified and syllabi developed, the program was presented to faculty within the School and the industry-based professional advisory team in order to garner feedback. Industry believed the curriculum content was appropriate (see Section V-C), and would lead to strong employment opportunities upon graduation. Industry also provided significant input regarding the software systems needed to deliver the program and helped identify areas that required more emphasis within the curriculum.

The discussion with the professional advisory team also covered the benefits, or otherwise, of certification. Clearly this is an area that varies from one segment of the computing industry to the next. However, it was clear that industry represented on the professional advisory team were having difficulties in hiring the right people in cybersecurity related positions and that they believed organizations that valued certification would train new employees as needed.

Certifications are available through many organizations, and have many different focuses. A non-exhaustive list includes:

- CompTIA Security+ [20],
- CompTIA CASP (Advanced Security Practitioner) [21],
- CCNA Security [22],
- CCNP Security [23],
- Certified Ethical Hacker [24],
- CISA (Certified Information Systems Auditor) [25],
- CISM (Certified Information Security Manager) [26],
- CISSP (Certified Information Systems Security Professional) [27],
- CCSP (Certified Cloud Systems Professional) [28],
- CSSLP (Certified Secure Software Lifecycle Professional) [29],
- GPEN (Global Information Assurance Certification Penetration Tester) [30], and
- OSCO (Offensive Security Certified Professional) [31].

Faculty developing the curriculum recognized that each certification course offered some benefit to the students, but decided to not follow any one certification pathway.

There are exemplar programs recognized through:

- National Centers of Academic Excellence in Cyber Defense (NSA and DHS) [32], and
- National Centers of Academic Excellence in Cyber Operations (NSA and DHS) [33].

It was felt by the faculty that designation as a Center of Excellence would be more valuable and more appropriate. However, there are strict requirements that must be met in order to be designated a Center of Excellence, and these include having generated graduates from the program. Therefore, designation as a Center of Excellence remains an aspirational goal of the program.

V. Current Status

A. Student Interest

Interest in the new program is strong. Inquiries from prospective students suggest that the program will reach its target initial enrollment with ease, and that these are mostly students that would not have come to Northwest Missouri State University in order to simply pursue a computer science degree. This net growth in undergraduate numbers was one of the goals of introducing the new cybersecurity degree. This growth is essential in the economic climate currently being experienced in Missouri, especially when combined with the anticipated decline in international graduate student numbers as a result of policy changes at the Federal level.

Within the university, there is also interest among students transferring from computer science into cybersecurity. This was anticipated, and one of the goals in developing the cybersecurity program was to facilitate movement of students between computer science and cybersecurity, especially in the first two years of study. Students are often not sure what they wish to study when starting at university and, as they better understand each discipline, their interests crystallize. In addition, the mathematics requirements for the computer science degree are more onerous and rigorous than they are for the cybersecurity degree and this is an important factor for students who find themselves struggling with mathematics. As a consequence of this internal interest in transferring into cybersecurity from computer science, the first two years of the cybersecurity degree will be offered in the 2018/19 academic year. Hence the first cybersecurity graduate should emerge in 2020/21.

B. Limited Faculty Resources

A challenge that the School of Computer Science and Information Systems is currently experiencing is a significant decline of international graduate students in the Masters of Applied Computer Science. This loss of revenue, compounded by the sharply declining financial support from the State, has resulted in a loss of four faculty lines in the School over the past two years. Hence, despite the introduction of a new program which necessitates the creation and delivery of new courses, there are no new resources coming into the School to support the program. This fiscal reality somewhat forced the School to develop a cybersecurity program that had as much overlap with the existing computer science degree as possible, while still achieving distinct program outcomes and preparing students for a different career path. Consequently, a major consideration in the identification of new courses was the presence of interest and expertise within the existing faculty. Resources were simply not available to develop new courses in new areas, even if that would have made the degree more attractive to incoming students.

C. Curriculum

As noted in Section IV, cybersecurity could be taught in many different ways with varying degrees of emphasis on the eight core knowledge areas. Circumstances within the institution and the State pushed Northwest Missouri State University to leverage existing courses and strengths, rather than developing new areas of expertise within the School. Consequently, the existing computer science degree was leveraged to the maximum extent possible in the creation of the new cybersecurity degree. However, each degree must have its own unique program outcomes and to distinguish cybersecurity from computer science five new cybersecurity related courses were added.

- Introduction to Cybersecurity
- Secure Programming
- Incident Response and Cyber Risk Management
- Digital Forensics
- Ethical Hacking

Some existing classes are required in the cybersecurity degree:

- Professional Ethics
- General Psychology
- General Statistics
- Discrete Mathematics
- Computer Programming I
- Computer Programming II
- Data Structures
- IT Hardware and Software
- Network Fundamentals
- Computer Organization
- Database Systems
- Operating Systems
- Secure Systems Administration
- Applied Cryptography

Even though there is some overlap with the computer science degree, the two program have different required courses, including different required general elective requirements. At this stage all computer science courses are electives to the cybersecurity students and all cybersecurity courses are electives to computer science students, but no student can satisfy the degree requirements for both computer science and cybersecurity within the confines of a 4-year degree. Specifically, the number of electives available within each degree is insufficient to permit a student to take all the necessary classes from the other degree. In particular the programs differ in their mathematics and science requirements, and the cybersecurity degree requires a separate course on ethics (it is embedded in other computer science classes) and a course in psychology.

VI. Future Hopes, Dreams and Expectations

The program is off to a promising start, with incredible support throughout the university during development. Student interest is strong both from current students considering changing into the program and incoming students who will be arriving on campus in Fall, 2018. Faculty are on board, and development of course material is well under way.

Industry support has been extremely positive as well. Students following the emphasis plan and/or participating in the

cyber-defense team have already received internships and job offers based on their experience within the existing courses (Networking, Network Security, Applied Cryptography, and Secure Systems Administration) and discussions with professional advisory team members indicates that graduates from this program can expect high levels of interest from industry. The primary goal over the next year is to build course content, nurture new enrollments and continue to maximize program visibility among both prospective students and employers.

A cybersecurity minor has also been proposed, and approved, providing a pathway for students from other areas of study to dip into the field as part of their academic program. Finding ways to broaden the appeal to students from a variety of fields will continue to be an active goal. Areas with immediate connections would include Criminology, Computer Science and Management Information Systems.

Long-term aspirations involve pursuing recongnition as a National Security Agency recognized Center for Academic Excellence [32] [33] and potentially seeking funding for students from programs such as the National Science Foundation's Cybercorps: Scholarship for Service [34]. By following suggested curricular practices and guidelines, these pathways will be available as the program matures over the next few years. Continued evolution of the curriculum, facilities and classroom resources is also expected as faculty and students grow with the new program.

VII. Conclusion

Northwest Missouri State University has introduced a cybersecurity degree that best takes advantage of the existing faculty interests and strengths while simultaneously addressing the emerging cybersecurity program recommendations [11]. This has meant leveraging the existing computer science degree and pursuing a focus in cybersecurity that builds on core computer science competencies (programming, operating systems, databases) in order to build a program which should lead to high-demand, well-paying, jobs. Industry has offered support and guidance in developing the program through participation at the industry advisory board meetings held annually.

Cybersecurity, like computer science, is a rapidly changing field. Risks and threats change constantly and software developers must remain current and be resilient to new attacks. It is likely that machine learning and artificial intelligence courses will be applied to the cybersecurity degree in the near future. These topics act as a disruptive technology with the potential to identify new threats and neutralize them. The program described here is adaptable and expected to morph and grow as the field does.

Acknowledgment

The authors would like to thank the faculty members that helped develop the cybersecurity program at Northwest Missouri State University: Joni Adkins, Doug Hawley, Charitha Hettiarachchi, Zhengrui Qin, Carol Spradling, and Cindy Tu.

References

[1] Kaspersky Labs, "A brief history of hacking," 2018, accessed: April 17, 2018. [Online]. Available: https://securelist.com/threats/a-brief-history-of-hacking/

[2] The Mentor, "The conscience of a hacker," *Phrack, Inc.*, vol. 1, no. 7, Phile 3 of 10, accessed: April 19, 2018. [Online]. Available: http://www.phrack.org/archives/issues/7/3.txt

[3] Wikipedia, "List of data breeches," 2018, accessed: April 17, 2018. [Online]. Available: https://en.wikipedia.org/wiki/List_of_data_breaches/

[4] ——, "WannaCry ransomware attack," 2018, accessed: April 17, 2018. [Online]. Available: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

[5] Lloyd's of London, "Counting the cost, cyber exposure decoded," 2017. [Online]. Available: https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/countingthecost

[6] Ponemon Institute, "2017 cost of data breech study," Ponemon Institute, Tech. Rep., June 2017, accessed: April 19, 2018. [Online]. Available: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN\&

[7] S. Morgan, "Cyber crime costs projected to reach $2 trillion by 2019," accessed: April 17, 2018. [Online]. Available: https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/\#4e610ed3a913

[8] Juniper Research, "Cybercrime will cost businesses over $2 trillion by 2019," accessed: April 17, 2018. [Online]. Available: https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

[9] Cyber Education Project, "Cyber education project website," 2018, accessed: April 17, 2018. [Online]. Available: https://www.cybereducationproject.org/

[10] ACM/IEEE-CS Joint Task Force on Computing Curricula, "Computer science curricula 2013," ACM Press and IEEE Computer Society Press, Tech. Rep., December 2013, accessed: November 14, 2017. [Online]. Available: http://dx.doi.org/10.1145/2534860

[11] ——, "Cybersecurity curricula 2017," ACM, IEEE Computer Society, AIS, and IFIP, Tech. Rep., December 2017, accessed: March 30, 2018. [Online]. Available: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

[12] ABET, Inc., "Criteria for accrediting computing programs, effective for review during the 2019-20 accreditation cycle," 2017, accessed: November 14, 2017. [Online]. Available: http://www.abet.org/wp-content/uploads/2017/11/CAC-Criteria-Version-2.0-2018-19.pdf

[13] ——, "Proposed criteria for cybersecurity and similarly named programs," 2018, accessed: April 17, 2018. [Online]. Available: https://www.surveymonkey.com/r/cybersecuritycriteria

[14] C. Willis, "Outcomes of advertised computer science faculty searches for 2017," 2017. [Online]. Available: http://web.cs.wpi.edu/~cew/papers/outcomes17.pdf

[15] Department of Labor, Bureau of Labor Statistics, "Occupational outlook handbook, information security analysts," 2017, accessed April 17, 2018. [Online]. Available: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

[16] S. Morgan, "One million cybersecurity job openings in 2016," *Forbes Magazine*, accessed: April 19, 2018. [Online]. Available: https://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#3cb5b87f27ea

[17] ——, "Zero-percent cybersecurity unemployment, 1 million jobs unfilled," *Cybersecurity Business Report*, accessed: April 19, 2018. [Online]. Available: https://www.csoonline.com/article/3120998/techology-business/zero-percent-cybersecurity-unemployment-1-million-jobs-unfilled.html

[18] ACM/IEEE-CS Joint Task Force on Information Technology Curricula, "Information technology curricula 2017," ACM Press and IEEE Computer Society Press, Tech. Rep., December 2017, accessed: June 21, 2018. [Online]. Available: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/it2017.pdf

[19] J. J. Ekstrom, B. M. Lunt, A. Parrish, R. K. Raj, and E. Sobiesk, "Information technology as a cyber science," in *Proceedings of the 37th SIGITE technical symposium on Information Technology education (SIGITE '17)*. New York: ACM, October 2017, pp. 84–89.

[20] CompTIA, "Comp TIA security+," 2018, accessed April 17, 2018. [Online]. Available: https://certification.comptia.org/certifications/security

[21] ——, "Comp TIA advanced security practitioner," 2018, accessed April 17, 2018. [Online]. Available: https://certification.comptia.org/certifications/comptia-advanced-security-practitioner
[22] CISCO, "CCNA security," 2018, accessed April 17, 2018. [Online]. Available: https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-security.html
[23] ——, "CCNP security," 2018, accessed April 17, 2018. [Online]. Available: https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/professional/ccnp-security.html
[24] EC-Council, "Certified ethical hacker," 2018, accessed April 17, 2018. [Online]. Available: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/
[25] ISACA, "Certified information systems auditor," 2018, accessed April 17, 2018. [Online]. Available: http://www.isaca.org/certification/cisa-certified-information-systems-auditor/pages/default.aspx
[26] ——, "Certified information security manager," 2018, accessed April 17, 2018. [Online]. Available: http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx
[27] $(ISC)^2$, "Certified information systems security professional," 2018, accessed April 17, 2018. [Online]. Available: https://www.isc2.org/Certifications/CISSP\#
[28] ——, "Certified cloud security professional," 2018, accessed April 17, 2018. [Online]. Available: https://www.isc2.org/Certifications/CCSP
[29] ——, "Certified secure software lifecycle professional," 2018, accessed April 17, 2018. [Online]. Available: https://www.isc2.org/Certifications/CSSLP
[30] Cyber Security & Information Systems Information Analysis Center (CSIAC), "GIAC penetration tester (GPEN)," 2018, accessed April 17, 2018. [Online]. Available: https://www.csiac.org/certification/giac-penetration-tester-gpen/
[31] Offensive Security, "Offensive security certified professional," 2018, accessed April 17, 2018. [Online]. Available: https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/
[32] NSA, "National centers of academic excellence in cyber defense," 2016, accessed April 17, 2018. [Online]. Available: 20186://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/
[33] ——, "National centers of academic excellence in cyber operations," 2016, accessed April 17, 2018. [Online]. Available: https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations/
[34] NSF, "Cybercorps: Scholarship for service," accessed April 30, 2018. [Online]. Available: https://www.sfs.opm.gov/