Issues in Information Systems
Volume 22, Issue 2, pp. 210-222, 2021

DOI: https://doi.org/10.48009/2_iis_2021_221-233

Cybersecurity student talent recruitment and development: A case study

Ping Wang, *Robert Morris University, wangp@rmu.edu*

Abstract

There is a substantial and fast-growing workforce demand for qualified cybersecurity professionals to defend our cyber space and critical assets against growing cyber threats and attacks. Cybersecurity is a highly technical, comprehensive, and multi-disciplinary field, and it is a challenging task to recruit and develop cyber talent that meet the high expectations of the field. The national Centers of Academic Excellence in Cyber Defense Education (CAE-CDE) designation by the U.S. National Security Agency and Department of Homeland Security (NSA/DHS) is a high-quality program that promotes excellence in cybersecurity education for developing cyber talent. CAE-CDE schools in good standing are eligible for government funding such as the Department of Defense Cyber Scholarship Program (DoD CySP) to recruit and develop cybersecurity talent for DoD agencies and to enhance the national pipeline for cybersecurity professionals. This research presents an effective approach to cyber talent recruitment and development using the case study of a DoD CySP program at a CAE-CDE designated university.

Keywords: Cyber talent, CAE-CDE, DoD CySP, scholarship, recruitment, development, mentoring

Introduction

There is a substantial and fast-growing workforce demand for better educated and qualified cybersecurity professionals to defend our cyber space and critical assets against various cyber threats and attacks (U.S. Department of Labor BLS, 2021; Wang & Sbeit, 2020). Meanwhile, there is inadequate supply of cybersecurity professionals for the growing demand. A recent workforce survey study conducted by the non-profit $(ISC)^2$, the International Information System Security Certification Consortium, indicates that the shortage of cybersecurity professionals is approximately three million around the world and about half a million in North America and that the majority of the subject organizations reported concerns of moderate or extreme risks of cybersecurity attacks due to insufficient cybersecurity staff ($(ISC)^2$, 2018). Therefore, it is a significant issue to identify, recruit, and develop adequate and qualified cyber talent for the workforce.

Quality education and training programs are a gateway to qualified workforce. A credible quality assurance system is needed to evaluate and maintain program outcomes and quality of cybersecurity education and training providers. In the United States, the national Centers of Academic Excellence in Cyber Defense Education (CAE-CDE) designation program jointly sponsored by the National Security Agency (NSA) and Department of Homeland Security (DHS) has been the most comprehensive and reputable national standard for the field of cybersecurity education, which evaluates and certifies cybersecurity education programs with comprehensive and measurable criteria for program evaluation and specific knowledge units and outcomes for assessment (Wang, Dawson, & Williams, 2018). CAE-CDE schools are also eligible for

federal funding resources, such as the Department of Defense Cyber Scholarship Program (DoD CySP) for recruitment and development of cyber talent for the DoD cyber workforce.

Cybersecurity is a multidisciplinary and challenging field (Blair, Hall, & Sobiesk, 2019). It is not only highly technical but also a sophisticated field that involves computer information systems, computer science, application technology, business management, communication, critical thinking, problem-solving, and analytical skills. Effective approaches are needed to identify and recruit cyber talent to prepare them for the career field. In addition, as college students often lack the practical experience needed for the field, professional mentoring should be an integral component in students' learning at cybersecurity programs (Dean, 2019; Wang & Sbeit, 2020). This research paper shares an approach to effective recruitment and a mentoring model for cyber talent development based on a case study of a current cyber scholarship program at a private university in the northeast of the United States. The follow sections of the paper present the relevant background, the recruitment approach and the mentoring model used for the case study, and discusses the implementation process and findings.

Background

Student interest means that the student is willing and motivated to pursue advanced study and training in a certain field. Student interest is measured by the student admissions to and enrollment in the program of study. Research shows that that student interest in Cybersecurity is positively affected and motivated by promising and rewarding careers in the cybersecurity industry and reputable programs with good quality curriculum and courses for cybersecurity education (Aufman & Wang, 2019). As an implication, an effective approach to cyber talent recruitment should appeal to student potential and interest with realistic rewards of the career field and reputable curriculum and courses of the educational program.

The Cybersecurity Industry Model published by the U.S. Department of Labor highlights comprehensive tiers of competencies or clusters of knowledge, skills, and abilities (KSAs) needed for cybersecurity professionals (US Department of Labor, 2014). The five tiers of competencies are:

- Tier 1 refers to Personal Effectiveness Competencies or essential personal attributes that include interpersonal skills, ethical integrity and professionalism, and lifelong learning commitment.
- Tier 2 refers to Academic Competencies that include well-rounded academic proficiencies as well as communication, critical and analytical thinking and fundamental IT user skills.
- Tier 3 refers to Workplace Competencies that include teamwork, planning and organizing, creative thinking, problem solving and decision making and business fundamentals.
- Tier 4 refers to Industry-wide Technical Competencies that include KSAs in cybersecurity technology, risk management, and incident response and remediation.
- Tier 5 covers the Industry-sector Functional Areas including security provision system, security operation and maintenance, protection and defense from threats, threat investigation, information collection and analysis, and cybersecurity governance.

Tier 1 through Tier 3 are foundational work readiness skills demanded by most employers. Tier 4 and Tier 5 are industry-specific competencies. The Management Competencies and Occupation-Specific Requirements at the top of the model represent the specialization and management skills for specific occupations. The tiers of competencies presented in this model incorporated many concepts, functional categories and KSAs from the NICE National Cybersecurity Workforce Framework (NICE, 2020). Therefore, cyber talent development should address comprehensive skills to prepare qualified professionals for the cybersecurity workforce.

Mentoring should be an integral part of cyber talent development in cybersecurity education to enable students to succeed academically and professionally. An effective mentoring relationship should inspire the mentees toward personal behavior emulation and modification for professional success. Dawson and Thomson (2018) proposed six key personal traits required for professional success in the future cybersecurity workforce:

(1) Systematic Thinkers – the future employees in cybersecurity need to have systematic and creative thinking about the problems, solutions and impacts in the context of the complexity and interconnectedness of the cyber domain.
(2) Team Players – the magnitude of complexity and interconnectedness of the cyber domain will demand cybersecurity professionals to work more in teams.
(3) Technical and Social Skills – future cyber workers should possess technical and social skills in order to work with human users and recognize human vulnerabilities in the cyber domain.
(4) Civic Duty – cybersecurity professionals should have ethical commitment to their organizations and the national security to minimize insider threats.
(5) Continued Learning – the future cybersecurity professionals need to have a passion for learning new knowledge and problem-solving skills as technology changes rapidly.
(6) Communications – cybersecurity professionals should be able to communicate technical and non-technical subjects effectively with various colleagues and partners.

Therefore, a cybersecurity program should provide excellent curriculum, courses, support resources as well as rewarding career opportunities to attract and recruit cyber talent. To prepare students for the cyber workforce, comprehensive mentoring should be provided for cyber students to develop academic and professional readiness.

Case Study

This research uses the case study methodology to present and illustrate an approach to cyber talent recruitment and development approach. The case study is based on the implementation of recruitment and development of cyber talent for the DoD CySP grant program at Robert Morris University (RMU) in the northeast of the United States. The case study highlights the cybersecurity program quality, the cyber talent recruitment approach, and the comprehensive mentoring approach for student success.

RMU is a nationally ranked, selective, and non-profit private university located in Pittsburgh, PA. RMU is accredited by the Middle States Commission on Higher Education to offer bachelor's, master's, integrated bachelor's/master's, and doctorate degree programs. RMU has a total enrollment of about 5,000 including over 800 graduate students. RMU provides high quality education in Cybersecurity and currently offers a Bachelor of Science degree program in Cybersecurity (previously known as Cyber Forensics and Information Security) as well as Master of Science degree programs in Cybersecurity and in Cyber Investigations and Intelligence. The university is a national Center of Academic Excellence in Cyber Defense Education (CAE-CDE) designated by the National Security Agency and Department of Homeland Security (NSA/DHS) and also holds three current ABET computing accreditations.

1. Curriculum & Learning Activities

The bachelor's and master's degree programs in Cybersecurity at RMU provide high quality and comprehensive curricular learning activities for all students to succeed academically and professionally. The programs and learning outcomes are mapped to the criteria and requirements for the CAE-CDE designation and ABET accreditation. The undergraduate program in Cybersecurity, is accredited by the ABET CAC (Computing Accreditation Commission). The CAE designation and ABET accreditation jointly indicate the excellence in cybersecurity education provided by RMU. In addition, the student learning outcomes from the cybersecurity programs embrace and satisfy all the six competency areas expected by the DoD CySP program, which include knowledge of cybersecurity techniques, knowledge of human factors in cybersecurity, and skills and abilities for critical and analytical thinking, problem solving, decision making, and verbal and written communication. These competencies are reasonable expectations for the cybersecurity professionals also recognized and emphasized in the US Department of Cybersecurity Industry Model and the NICE Cybersecurity Workforce Framework.

The Bachelor of Science (BS) degree program in Cybersecurity (formerly known as Cyber Forensics and Information Security) is a well-designed 123-credit program accredited by ABET and consists of the following technical and comprehensive curricular components: (1) 39 credits of RMU Core including math, sciences, arts, humanities and communication to give students a well-rounded college education; (2) 33 credits of Major courses including at least two levels of programming languages such as Python, Java, C++, C#, networking, operating systems, database systems, system analysis, fundamentals of information technology security, and social and ethical issues of computing; (3) 21 credits of Cybersecurity or Digital Forensics Concentration courses, such as computer network security, digital forensics, cyber law, IT security and assurance, ethical hacking, mobile security and forensics, intrusion detection and network forensics; (4) 15 credits of Area of Interest that include options of 5 interrelated courses in a secondary area supporting the student's primary interest; and (5) 15 credits of Open Electives for the student's open exploration among any credit courses at the university. The Master of Science (MS) degree programs in Cybersecurity require at least 30 credits of graduate level course work with a relevant undergraduate degree as a prerequisite. The MS degree programs emphasize more specialized and in-depth studies including core courses in the subject areas of operating systems, network technology and management, database management systems, network security, secure programming, advanced cybersecurity topics, and a capstone project.

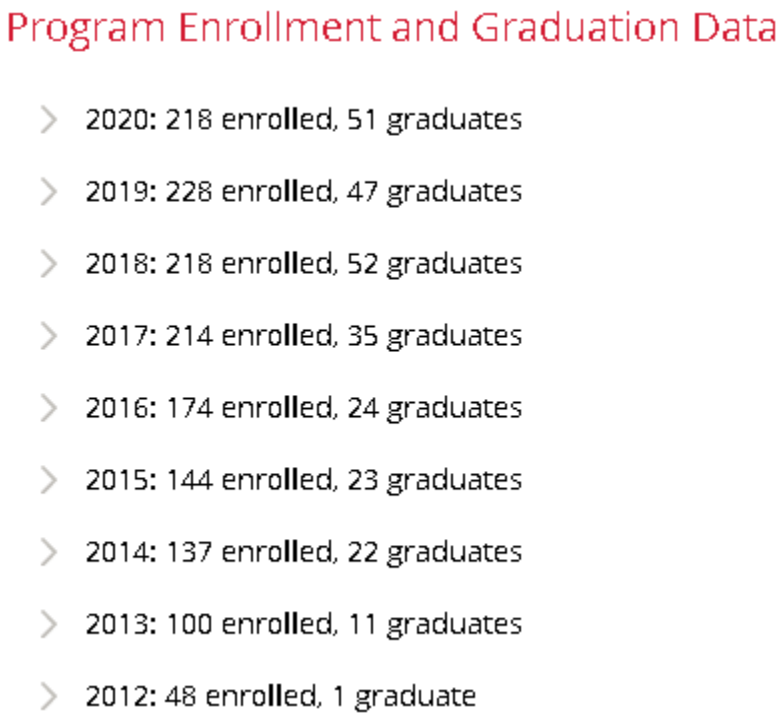

Figure 1. RMU Cybersecurity Enrollment and Graduation Data

The integrated BS/MS degree option allows undergraduate students to pursue their master's degree at an accelerated pace usually in 5 years, including 4 years of undergraduate and 1 year of graduate study. The integrated BS/MS program consists of an undergraduate degree, such as BS in cybersecurity, and a MS degree such as in cybersecurity, cyber investigations, or data analytics. The integrated program in Cybersecurity has been popular with a steadily increasing student population, which is a healthy pool for CySP candidate recruitment and selection. Figure 1 above shows the BS Cybersecurity program enrollment and graduation data, which includes integrated cybersecurity students.

Cybersecurity education should involve multi-disciplinary teaching and learning activities as cyber professionals need to develop and possess both technical and non-technical competencies and knowledge, skills, and abilities (KSAs), such as critical and analytical thinking, problem solving, communication, teamwork and leadership skills expected for the future cyber workforce. RMU recognizes the technical and multi-disciplinary KSAs required for successful cybersecurity professionals. In addition to the comprehensive curriculum and course offerings and requirements at the undergraduate and graduate levels, the course work provides comprehensive and a variety of learning activities and experience for students to obtain technical and non-technical KSAs. The learning activities in the courses include extensive hands-on work using technology, interactive lectures and discussions, collaborative team projects and presentations, and individual research project and presentations. These comprehensive course activities along with rich extra-curricular activities jointly help students to develop technical and non-technical competencies and KSAs, such as critical and analytical thinking, problem solving, communication, teamwork and leadership skills expected for the future cyber workforce.

2. CYBER TALENT RECRUITMENT APPROACH

Recruiting talented students is a critical first step to the success of preparation and development of cyber professionals. In addition to the appeal of the cybersecurity career field and program quality, cyber talent recruitment needs a well-organized process to be effective. RMU has established and successfully implemented a systematic approach to student recruitment for the DoD CySP program. The approach is based on the AAA Model (Advertise, Assist, and Assess) as shown in Figure 2 below and successfully tested in the recruitment for CySP candidates in the past year.

Figure 2. The AAA Model for Cyber Talent Recruitment

The AAA Model for RMU's cyber talent recruitment for the CySP program consists of 3 sequential components: Advertise, Assist and Assess.

- ***Advertise*** is to actively spread the news and information of the CySP program within the university community by various means to promote awareness of the program and its benefits and requirements and to increase the potential student interest and candidate pool.
- ***Assist*** is to provide assistance and guidance for interested students and applicants to fully understand the program and complete necessary application requirements and paperwork.
- ***Assess*** is to evaluate student applications and supporting documents and come up with a specific recommendation for each applicant according to the requirements and expectations of the DoD CySP program. RMU has successfully implemented the 3 components of the AAA model for student recruitment as the first step of the CySP program. The Principal Investigator (PI) of the grant program will continue the research to enhance the process for cyber talent recruitment, retention, and development.

RMU has effectively implemented the AAA model in the cyber talent recruitment for the CySP program. The following summarizes the implementations of the three elements of the model.

Advertise

RMU has actively advertised the CySP program in the campus community and to relevant student populations. Specifically, RMU has actively promoted awareness of and interest in the CySP program by the following means of advertising.

- The PI of the program and POC (Point of Contact) for RMU's CAE-CDE created and updated a public information web page on the CySP program. The web page includes a summary of the program, scholarship award benefits, minimum requirements and a link to more detailed application background and requirements, instructions on how to apply along with the new student

application form and resume template, the schedule of an upcoming virtual information session on Google Meet, and contact information. This web page was on the RMU web domain and visible to all students, faculty, and staff of the RMU community and partners and has effectively generated frequent interest and inquiries about the program.

- Digital flyers about the CySP program were created and sent by email to all eligible undergraduate and graduate students at RMU.
- The CySP program information was also shared with interested cybersecurity program faculty and staff at RMU to spread the word to their students in classrooms and through postings at Blackboard course sites.
- The department of Computer and Information Systems and its hosting school where cybersecurity programs are housed were made aware of the CySP and provided great support.
- To accommodate safety during the Covid-19 pandemic, the PI of the CySP program and RMU's CAE POC hosted a virtual information session on Google Meet to present important program information, guidelines for application, and answer student questions on the program. A total of 23 students attended the session, indicating a fairly strong interest among the student population.

Assist

DoD CySP is a fairly new program to RMU and has a number of detailed requirements. It is necessary to provide assistance and guidance for interested students and applicants to fully understand the requirements and obligations and complete their application paperwork. RMU has provided the following assistance to interested students and applicants:

- The program PI has talked with individual students interested in the program virtually via Google Meet video conferencing or by phone to discuss their interest, background, education, career plans, and plans and questions for applying for the scholarship.
- As part of the project team, the staff from the Office of Scholar Development had individual appointments with individual student applicants virtually to help them complete their application forms and provide professional communication guidance on formatting and editing their resumes and personal statement of competencies per expectations for the CySP program.
- The program PI answered frequent email inquiries from students regarding the CySP requirements for applicant eligibility, graduation dates, transcripts, recommendation letters, statement of competencies, resumes, security clearance, and benefits and obligations for the CySP scholarship.
- Several faculty members of the cybersecurity program provided recommendations letters for students as part of their application documentation.

Assess

To help identify qualified candidates for the CySP program, RMU is responsible for assessing the applicants and making initial recommendations to the DoD CySP program office. RMU has carefully planned and completed the assessment of student applications in the following steps:

- An Assessment Committee with representatives from the cybersecurity program and the office of Scholar Development reviewed, evaluated, and discussed the student applications.
- The Assessment Committee carefully reviewed and discussed each application form and the applicant's official transcripts, resume, list of awards, honors and distinctions, reference letters, and competency statement.

- The committee met to discuss their evaluations of each applicant on the six items of knowledge, skills and attributes for the CySP program, and they discussed their rationale for the scores and the type of recommendation.
- The committee provided input on the final recommendations of the applicants based on their assessment and discussions of their application materials.
- The program PI and RMU institutional representative/grant officer submitted the committee recommendations on the applicants along with their complete application packages to the DoD CySP program office by the due date.
- During the application processing at RMU, all student applications materials and private information were safe-guarded and only shared with personnel who has the need to know. Applicants were also pre-warned not to publicize the DoD employer according to the program policy.

3. Comprehensive Mentoring Approach for Student Success

Student success in the context of cybersecurity education is defined as reaching both academic and professional goals with acquisition of necessary knowledge, skills, and abilities. Student success in cybersecurity education during the CySP scholarship period is essential to the success of their future professional service for public or private employers. RMU provides high quality program, courses and learning activities as well as comprehensive mentoring to enable cyber talent to succeed academically and professionally.

Comprehensive Mentoring Model

RMU provides comprehensive and dedicated mentoring to help students selected for the CySP program to succeed academically and professionally and be ready for their cybersecurity professional assignment and service upon graduation. Recognizing the comprehensive and multi-disciplinary nature of cybersecurity, the CySP program at RMU has adopted and implements the Comprehensive Mentoring Model for Cybersecurity Education in Figure 3 below to help students of the program to succeed academically and professionally. The PI of the CySP program at RMU serves as the primary faculty mentor conducting regular mentoring activities in the following areas of the model: Academic Mentoring, Career Guidance, Extra-Curricular Mentoring, and Ethical Guidance. The program PI will work with relevant offices, staff, and other faculty members for any necessary assistance. A Blackboard learning shell is used to mentor the students with regular learning activities and submissions of progress reports, including during the regular semesters and the summer. The Blackboard mentoring site contains important mentoring materials and presentations on government service policies, requirements and ethics. Students receive regular feedback and advice on their progress in academic, professional and extra-curricular activities via Blackboard and email interactions with the faculty mentor.

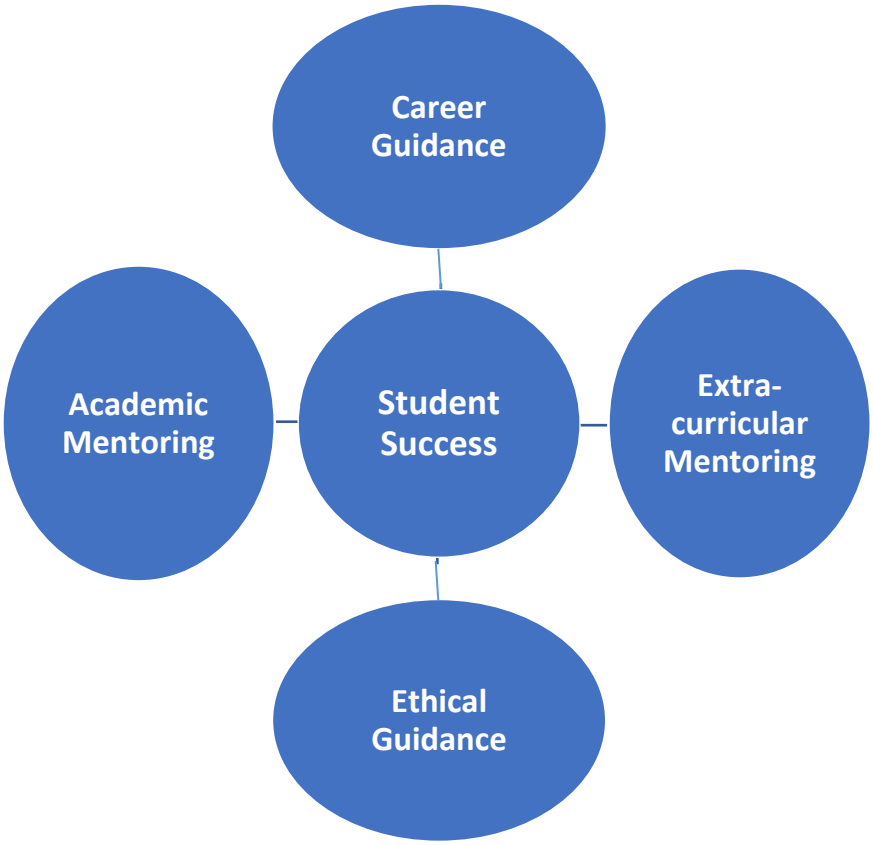

Figure 3. Comprehensive Mentoring Model for Cybersecurity Education (Wang & Sbeit, 2020)

Student success is the center and goal of the comprehensive mentoring model, which includes the student's successful achievements of the academic goal and the professional goal. The academic goal is to complete the program and course requirements for graduation and acquire technical and non-technical competencies and KSAs for the cyber field. The professional goal is to enter the desired professional field – or honor the commitment to DoD cyber service for the CySP program with academic and professional readiness. Professional mentoring for the students is instrumental in keeping everyone on track for graduation with continued excellence and readiness for starting and fulfilling their service to the government employers.

Academic Mentoring

Each cyber scholar in the program receives regular academic mentoring during the scholarship period. Academic mentoring in cybersecurity education is to provide regular one-on-one or group contacts, meetings and communication between the mentor and student mentees to monitor mentees' academic progress, provide timely advice, and address academic questions. Academic mentoring activities and communication include the following topics:

- Course selection for registration
- Time management
- Course-related technical questions

- Cybersecurity software tools
- Cybersecurity study resources
- Recommendations for further research
- Cybersecurity research methods and opportunities

Career Guidance

The cyber students of the CySP program receive regular career guidance during the scholarship period. The Career Guidance component is to advise and guide students in cybersecurity career opportunities and preparation for the professional field, including professional certifications. Students benefit from the mentoring and guidance in the following areas:

- Cybersecurity job titles and duties
- Qualifications and expectations for various cyber positions
- Cybersecurity workforce trends and needs for continuous learning
- Guest lectures and practitioner speaker opportunities
- Expectations and suggestions for internships
- Full-time cyber jobs and recommendations
- Professional contacts and networks in the cyber field
- Professional certifications and their value
- Professional groups and memberships in the cyber field
- Tips for job relocation

Extra-curricular Mentoring

The students of the CySP program also receive regular mentoring on extra-curricular learning during the scholarship period. The Extra-curricular Mentoring component in the comprehensive mentoring model is to guide and facilitate students' learning through activities outside classrooms. The out-of-classroom learning activities may occur in a variety of format, and guidance, advice and recommendations from faculty and practitioner mentors are very helpful. The extra-curricular learning and mentoring may include the following activities that have been used at RMU:

- Service-learning projects
- Cybersecurity competitions
- Cybersecurity conferences
- Cybersecurity games
- Field trips and visits
- Interviews with industry practitioners
- Sponsored research projects

The service-learning activities may involve volunteer or co-op service that provides students valuable experience to apply their classroom learning to the real world, develop their sense of responsibility for service, and enhance their interest in the cybersecurity field (Wang, 2015).

Ethical Guidance

Finally, each CySP student also receives regular mentoring on ethical guidance during the scholarship period. The Ethical Guidance component in the comprehensive mentoring model requires that the mentor serve as a role model and educate student mentees toward professional and ethical behavior for honorable service. Ethical guidance is especially important for students who will be serving in the sensitive cybersecurity areas with government agencies. Guidance on legal and ethical behavior also helps to prevent insider attacks, which is critical to the success of overall cybersecurity for an organization and nation and to the success of individual cyber workers (Dawson & Thomson, 2018). Ethics education should be integrated across the entire computing education including security and privacy programs to train students to be responsible users of technology (Grosz et al., 2019). Mentoring in ethics may involve the presentations, readings, and discussions on the following topics:

- Ethical professional behavior for IT and cyber workforce
- The role of cybersecurity and cyber intelligence in national security
- The importance of authorization in penetration testing
- Data security and privacy laws
- Compliance and reporting requirements
- Non-disclosure agreement
- Security clearance requirements
- Conflict of interest disclosures
- Copyright protection and plagiarism
- Ethics in cybersecurity research

The program PI meets or communicates with CySP students on a regular basis to check their academic progress and provide mentoring in the areas above. In case physical meetings are not possible due to emergencies, weather, travel or student internships, virtual meetings and communication such as phone and/or email discussions will be conducted instead.

Conclusion

There is a shortage of and an increasing demand for qualified cybersecurity professionals. Recruiting and developing qualified cyber professionals is critical to meeting the demand through cybersecurity education and training. Quality program curriculum and courses and an effective recruitment process are essential to successful cyber talent recruitment. Regular mentoring of cyber students is important for them to succeed academically and professionally to be ready for the cyber workforce.

This research paper presents a case study of a cyber scholarship program at a U.S. university to illustrate an effective approach to cyber talent recruitment and a comprehensive mentoring model for student success. The cybersecurity program in the case study maintains excellence in cyber defense education with both CAE-CDE designation and ABET CAC accreditation and implements a well-organized process to advertise the program, assist student applicants in their exploration, and assess the candidates for program recommendation and selection. The program also adopts and implements a comprehensive mentoring model that includes academic mentoring, career guidance, extra-curricula mentoring, and ethical guidance to help students toward successful completion of their program and professional readiness for government service. The cyber program has been ongoing with successful student progress on target to graduation and completion of the program at RMU to transition to their internships and employment with government

employers. The positive outcome indicates the general effectiveness of the practices discussed above on student recruitment process and the mentoring approaching in cyber talent development.

However, this is a new program to RMU and there are lessons learned. First, the main issue in the feedback from the students of the cyber scholarship program is that the scholarship distribution process needs to be improved. For example, issuing and mailing paper checks of monthly living stipend to students should be replaced with direct electronic deposits, which is faster and more secure than U.S. mail and more convenient for students who are away from their home address for summer internships. Second, more involvement of partnerships from government employers in the mentoring process would be better for cyber students of the program to have more exposure and experience with the cybersecurity service expectations for government service. This case study is only preliminary and limited. Future studies may include more student data and new variables, such as the use of industry and government partnerships in mentoring, which may impact the student recruitment and development processes.

Acknowledgement:
This research was supported by a grant from the U.S. Department of Defense (Grant#: H98230-20-1-0352).

References

(ISC)2. (2018). Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens: (ISC)2 Cybersecurity Workforce Study 2018. Retrieved from https://www.isc2.org/research

Aufman, S., & Wang, P. (2019). Discovering student interest and talent in graduate cybersecurity education. In S. Latifi (Eds.), *Advances in Intelligent Systems and Computing* (pp.77-83). Springer Nature Switzerland AG.

Blair, J.R.S., Hall, A.O., & Sobiesk, E. (2019). Educating future multidisciplinary cybersecurity teams. *Computer,* March 2019. 58-66.

Dawson, J., & Thomson, R. (2018). The future of cybersecurity workforce: Going beyond technical skills for cyber performance. *Frontiers in Psychology, vol* 9 (744). 1-12.

Dean, K. (2019). What everybody ought to know about mentoring in InfoSec. AT&T Cybersecurity. Retrieved from https://www.alienvault.com/blogs/security-essentials/what-everybody-ought-to-know-about-mentoring-in-infosec

Grosz et al. (2019). Embedded ethics: Integrating ethics across CS education. *Communications of the ACM, 62*(8), 54-61.

NICE (National Initiative for Cybersecurity Education), NIST (National Institute of Standards and Technology. (2020). NICE Cybersecurity Workforce Framework (SP800-181 Revision 1). Retrieved from https://doi.org/10.6028/NIST.SP.800-181r1

US Department of Labor. (2014). Cybersecurity Industry Model. Retrieved from www.doleta.gov

U.S. Department of Labor BLS (Bureau of Labor Statistics). (2021). Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Wang, P. (2015). Project-based curricular service learning for cybersecurity education. *National Cybersecurity Institute Journal, 2*(3). 5-12.

Wang, P., Dawson, M., & Williams, K.L. (2018). Improving cyber defense education through national standard alignment: Case studies. International Journal of Hyperconnectivity and Internet of Things. 2(1), 12-28.

Wang, P., Hayes, N., Bertocci, M., Williams, K., & Sbeit, R. (2020). The role of industry partnerships and collaborations in information technology education. *ITNG2020, Advances in Intelligent Systems and Computing, 1134* (pp.9-15). Springer Nature Switzerland.

Wang, P., & Sbeit, R. (2020). A comprehensive mentoring model for cybersecurity education. In S. Latifi (Eds.), *Advances in Intelligent Systems and Computing* (17-23). Springer Nature Switzerland AG.