Cybersecurity Program Accreditation: Benefits and Challenges

Rajendra K. Raj
Rochester Institute of Technology
Rochester, New York, USA
rkr@cs.rit.edu

Vijay Anand
Southeast Missouri State University
Cape Girardeau, Missouri, USA
vanand@semo.edu

David Gibson
United States Air Force Academy
Colorado Springs, Colorado, USA
david.gibson@usafa.edu

Siddharth Kaza
Towson University
Towson, Maryland, USA
SKaza@towson.edu

Andrew Phillips
United States Naval Academy
Annapolis, Maryland, USA
aphillips@usna.edu

ABSTRACT

The Curricular Guidelines for Post-Secondary Degree Programs in Cybersecurity (CSEC 2017) released by the Joint Task Force of the ACM, IEEE Computer Society, AIS and IFIP have begun to define the academic field of cybersecurity. Increasing numbers of institutions are now offering full-fledged undergraduate cybersecurity degree programs. However, as the CSEC 2017 guidelines do not define what constitutes a standalone undergraduate cybersecurity degree, the computing community needs to agree on parameters of what such a degree ought to be. To this end, ABET has created flexible accreditation criteria for cybersecurity programs guided extensively by CSEC 2017 and community input. These criteria were used to conduct pilot accreditation visits of four distinct cybersecurity programs in 2017-18.

This panel discusses benefits, challenges, and costs of cybersecurity program accreditation. The panelists, who represent the first four ABET-accredited cybersecurity programs, will discuss major curricular features of their programs, their motivation for participating in the pilot accreditation, the effort in preparing for accreditation, and the benefits anticipated both for their programs and the larger computing community due to program accreditation.

CCS CONCEPTS

• **Social and professional topics** → **Accreditation; Model curricula; Computing education programs;**

KEYWORDS

Program accreditation, cybersecurity education, computer security education, information assurance education.

ACM Reference Format:

Rajendra K. Raj, Vijay Anand, David Gibson, Siddharth Kaza, and Andrew Phillips. 2019. Cybersecurity Program Accreditation: Benefits and Challenges. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education (SIGCSE '19), February 27-March 2, 2019, Minneapolis, MN, USA*. ACM, New York, NY, USA, 2 pages. <https://doi.org/10.1145/3287324.3287325>

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

SIGCSE '19, February 27-March 2, 2019, Minneapolis, MN, USA

© 2019 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-5890-3/19/02.

<https://doi.org/10.1145/3287324.3287325>

1 SUMMARY

The worldwide demand for cybersecurity professionals has been addressed by various training programs and specialized certificates for current practitioners. Designation as a National Center of Academic Excellence (CAE) in Cyber Defense or Cyber Operations [4] have helped US institutions get started in this space. With many institutions beginning to develop undergraduate cybersecurity programs, there is a need to establish cybersecurity as a formal academic discipline. Shared expectations of the core knowledge, skills, and abilities of cybersecurity program graduates will help institutions developing curricula and employers hiring graduates [3].

The CSEC 2017 [2] curricular guidelines from the Joint Task Force of the ACM, IEEE Computer Society, AIS, and IFIP describe different aspects of cybersecurity education, but do not define what constitutes an undergraduate cybersecurity program. To establish what constitutes an accreditable 4-year undergraduate cybersecurity degree program, the Computing Accreditation Commission (CAC) of ABET has developed accreditation criteria for cybersecurity degree programs based largely on the CSEC 2017 guidelines and community input [1]. ABET's approach provides flexibility for a variety of cybersecurity programs to meet the criteria, while supporting outcomes, quality, and continuous improvement.

For the first time, four cybersecurity programs were accredited by ABET in 2017-18. The panelists, who represent these first four ABET-accredited programs, will discuss unique aspects of their programs, their motivations for seeking accreditation, and challenges faced in creating accreditable programs. The panel continues the dialog of what constitutes a proper academic undergraduate cybersecurity program.

Table 1 outlines the panel structure. The moderator will introduce the panelists and briefly discuss the background cybersecurity education. The panelists' position statements are shown in the next section. Ample time is reserved for audience participation.

Table 1: Panel Structure

	Description	Duration
1	Introductions and Background	8 minutes
2	Panelists' Presentations	32 minutes
3	Audience Q & A	30 minutes
4	Summary	5 minutes

2 POSITION STATEMENTS

2.1 Rajendra K. Raj

Rajendra K. Raj, a professor of computer science at Rochester Institute of Technology, heads the department's security cluster. He co-chaired ABET's CAC criteria committee that created the new cybersecurity program criteria that will become official in 2019-20.

Raj will moderate the panel, introduce the panelists, and briefly outline the background in cybersecurity education leading to the ABET accreditation criteria for cybersecurity. He will also facilitate the audience Q & A and discussion, and summarize the session.

2.2 Vijay Anand

Vijay Anand is associate professor of computer science at Southeast Missouri State University and a member of the Missouri Governor's Cybersecurity Task Force. Moving from industry to academia, he established Southeast's Cybersecurity program in 2011. Anand's research interests include real-time adaptability of Trusted Platform Modules to evolving threats, process institutionalization and improvements of security frameworks, intrusion detection, secure data transfer, usable security and privacy concerns.

Anand will discuss distinct features of Southeast's cybersecurity degree program that emphasizes industry needs of cybersecurity. He will discuss the highly-technical, hands-on and comprehensive cybersecurity that is constantly evolving based on industry feedback. Anand will present the comprehensiveness of the curriculum, which covers technical (software, hardware, communication, and infrastructure), business processes, compliance and operational aspects, along with the infrastructure needed to support hands-on learning. He will also address the validation of Southeast's cybersecurity program through ABET accreditation.

2.3 David Gibson

David Gibson is Professor Emeritus of Computer Science at the United States Air Force Academy (USAFA). He led USAFA's Computer Science department for 14 years, and the development and operation of USAFA's cyber education, training, and research programs including establishment of the Cyber Science degree. Gibson has held positions at the National Security Agency and Cyber Command. An ABET volunteer for 18 years, he served on the Cyber Education Project and the CSEC 2017 Joint Task Force.

Gibson will discuss the evolution of USAFA's cyber program from its roots in computer science to the recent establishment of a distinct Cyber Science degree that is a technically-rigorous program that prepares graduates to serve as military officers conducting both offensive and defensive cyber operations and leading others in the same. Gibson will discuss the USAFA's Computer Science and Cyber Science programs, and compare the benefits and costs of program accreditation by ABET and designation by NSA as a National Center of Academic Excellence in Cyber Operations.

2.4 Siddharth Kaza

Sidd Kaza is Chairperson of Computer and Information Sciences at Towson University, Maryland. His interests lie in cybersecurity education, learning sciences, and application development. His projects under the Cyber4All umbrella (towson.edu/cyber4all) have

been funded by the National Science Foundation, Department of Defense, Maryland Higher Education Commission, and others. Kaza served on the CSEC 2017 Joint Task Force and serves on the advisory board of the CSEC2Y curricular guidelines.

Kaza will discuss distinct features of Towson's cybersecurity program that is strongly rooted in computer science. The program, also designated as a National Center of Excellence in Cyber Operations, is focused on technical rigor in network security, application software, reverse engineering, and cyber operations. The program has been the tip-of-the-spear at Towson and helps create an institutional environment that holds four other programs in cybersecurity. Kaza will highlight challenges in maintaining cutting-edge programs and retaining faculty, while adhering to accreditation and designation requirements.

2.5 Andrew Phillips

Andrew Phillips is Academic Dean and Provost at the United States Naval Academy (USNA). Responsible for leadership of all facets of the Naval Academy academic program, Phillips led the development of the Center for Cyber Security Studies and the majors in Cyber Operations. Phillips is a past President of the Computer Science Accreditation Board (CSAB) and a CSAB Fellow, and a Team Chair/Program Evaluator for both ABET and the Middle States Commission on Higher Education.

Phillips will discuss the distinct features of USNA's Cyber Operations program that was designed to acknowledge the growing demand for cyber expertise in the Navy and Marine Corps. In that warfare centric context, fusing both offensive and defensive disciplines together is essential to understanding cyberspace operations. Because of the focus on adversaries, on maintaining operations in the presences of risk and threats, and on offensive techniques, the newly created Cyber Science Department was given the latitude to create a truly interdisciplinary blend of both technical and non-technical course material. Each of the Cyber Science Department courses specifically focus on offensive capabilities and/or defensive strategies, with a holistic view of what can be done from a technical or capabilities perspective as well as the legal/ethical perspective and the social engineering/human factors aspect of the adversary.

ACKNOWLEDGEMENTS

Anand acknowledges the immense support provided to Southeast's cybersecurity program by both the current and former presidents of Southeast Missouri State University, Dr. Carlos Vargas and Dr. Kenneth Dobbins. Raj acknowledges support provided by the US National Science Foundation under Award No. DGE-1433736.

REFERENCES

- [1] ABET, Inc. 2018. Criteria for Accrediting Computing Programs. Effective for Review During the 2018-19 Accreditation Cycle. (2018). <http://www.abet.org/wp-content/uploads/2018/02/C001-18-19-CAC-Criteria-Version-2.0-updated-02-12-18.pdf> Accessed: November 6, 2018.
- [2] Joint Task Force on Cybersecurity Education. 2017. *Cybersecurity Curricula 2017*. Technical Report. ACM, IEEE-CS, AIS SIGSEC, and IFIP WG 11.8. DOI: <http://dx.doi.org/10.1145/3184594>
- [3] R. K. Raj and A. Parrish. 2018. Toward Standards in Undergraduate Cybersecurity Education in 2018. *Computer* 51, 2 (February 2018), 72–75. DOI: <http://dx.doi.org/10.1109/MC.2018.1451658>
- [4] US National Security Agency and the Department of Homeland Security. 2018. Centers of Academic Excellence in Cybersecurity. (2018). <https://www.nsa.gov/resources/educators/centers-academic-excellence> Accessed: November 6, 2018.