Association for Computing Machinery

Advancing Computing as a Science & Profession

NEWS RELEASE

Contacts: Jim Ormond
212-626-0505
ormond@hq.acm.org

Well-Trained Cybersecurity Pros Needed to Fill 1.8 Million Open Jobs

First-Ever Global Curriculum Guidelines Reflect Worldwide Demand for Qualified Professionals and Urgent Industry Needs

NEW YORK, NY, February 20, 2018 – After an extensive two-year process, a joint task force led by the Association for Computing Machinery (ACM) and the IEEE Computer Society (IEEE-CS) has released a first-ever set of global curricular recommendations in cybersecurity education. This new set of guidelines, Cybersecurity Education Curriculum (CSEC2017), is designed to be the leading resource for comprehensive cybersecurity curricular content at the post-secondary level. More than 320 advisors drawn from 35 different countries contributed to CSEC2017.

The growing dependence on the world's cyber infrastructure—which includes everything from banking and financial services, to critical infrastructures such as utility companies, to classified government documents, to the personal information of ordinary citizens—means that almost every aspect of the way we live in the digital age is vulnerable to cyberattack. As a consequence, the need for cybersecurity professionals has grown exponentially in the past 10 years and shows no signs of slowing. Government and non-government sources estimate that 1.8 million cybersecurity-related positions worldwide will go unfilled by the year 2022. In order to meet this demand, academic departments around the world are launching initiatives to establish new cybersecurity degree programs or add cybersecurity education onto existing degree programs.

"The field of cybersecurity is in its formative stages," explained CSEC2017 Joint Task Force Co-Chair Diana Burley, a professor at The George Washington University. "Wonderful career opportunities exist for people who are interested in working in cybersecurity. At the same time, because it is a new discipline, the term 'cybersecurity education' has meant different things to different people. As a result, many students graduating from cybersecurity programs often lack the requisite knowledge and skills needed to fit within an industry or government environment. Higher-education professionals around the world have urgently needed a unified framework to help develop coursework and degree programs. CSEC2017 provides that framework. By bringing together computing educators and industry professionals from around the world, we've forged a set first-of-its-kind curricular guidelines that will meet the needs of students, higher-education professionals, and industry hiring managers."

These inaugural guidelines were developed to help institutions structure cybersecurity programs with the twin goals of: 1) offering flexibility, to allow curricula to be tailored to type of institution (undergraduate, graduate, community college), and 2) offering guidelines that encompass the broad range of specializations and occupations within cybersecurity, rather than a single program type.

"Encouraging participation in the development of CSEC2017 from industry representatives strengthened the link between the curriculum guidance provided by CSEC2017 and the workforce needs," explained CSEC2017 Joint Task Force Co-Chair Matt Bishop, Co-Director, Computer Security Laboratory at the University of California, Davis. "Workforce implementation roadmaps survey the current and projected employment landscape and lay out the skills needed for the job roles that are open. Various governments around the world are effectively using these frameworks to develop their cybersecurity workforces. "

CSEC2017 is organized around eight key knowledge areas (KAs). These include Data Security, Software Security, Component Security, Connection Security, System Security, Human Security, Organizational Security, and Societal Security. Within each knowledge area, the curricula list specific essential concepts in which every graduate should be proficient. For example, within the Data Security KA, graduates are expected to demonstrate proficiency in essential concepts such as basic cryptography and data integrity and authentication. Within the Connection Security KA, graduates should demonstrate proficiency in essential concepts including connection and transmission attacks. At the more granular level, CSEC2017 guides educators in developing coursework by providing descriptors of topics that should be covered. For example, within the Access Control essential concept section of the Data Security KA, a topic descriptor lists several types of access controls to which students should be introduced.

With both the knowledge areas and essential concepts, the Curriculum outlines theoretical and conceptual knowledge essential to understanding the discipline, as well as opportunities for hands-on practice to gain proficiency. CSEC2017 also reflects the fact that cybersecurity is a specialization that students typically pursue after receiving an introduction to computing by studying in one of five main disciplines, including computer science, computer engineering, information systems, information technology, or software engineering. The Curriculum's Disciplinary Lens sections provide guidance to educators based on a student's core discipline, influencing the approach of cybersecurity coursework, depth of content and learning outcomes.

In addition to ACM and IEEE-CS, the CSEC2017 Joint Task Force included the Association for Information Systems Special Interest Group on Security (AIS SIGSEC) and the International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8).

About ACM

ACM, the Association for Computing Machinery www.acm.org, is the world's largest educational and scientific computing society, uniting computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.