Chapter 9
Cybersecurity Curricular Guidelines

Matt Bishop
University of California – Davis, USA

Diana Burley
The George Washington University, USA

Lynn A. Futcher
Nelson Mandela University, South Africa

ABSTRACT

The Cybersecurity Curricular Guidelines, a joint effort of the ACM, IEEE Computer Society, AIS SIGSAC, and IFIP WG 11.8, were created to provide developers of cybersecurity curricula with guidelines for material to include. The curricular guidelines have eight knowledge areas, broken down into knowledge units and topics. Underlying cross-cutting concepts provide linkages among the knowledge areas. Disciplinary lenses enable the developer to emphasize the knowledge units appropriate to the goals of the developed curricula. Each knowledge area also includes a list of essential concepts that all curricula should cover to an appropriate depth. The guidelines can be linked to workforce frameworks and certification criteria as well as academic curricula.

INTRODUCTION

The urgency of securing our information infrastructure is clear from the numerous compromises of personal data as well as from compromises of commercial and government information. A key part of this is securing the computing infrastructure, which consists of networks and computers in their various guises – the Internet, personal computers, laptops, servers, "smart" devices such as phones and sensors connected to the Internet — as well as the policies, procedures, and user and administrator interfaces controlling those components

Other chapters in this book cover the nature of threats, how the associated risks affect the proper handling of data and systems, and examples of notable compromises and their effects. The number and

DOI: 10.4018/978-1-5225-7847-5.ch009

rate of compromises demonstrate that cybersecurity has not yet been fully integrated into the development, deployment, operation, and retirement of computing and network systems. Academic institutions are introducing courses and programs to teach students about cybersecurity. The topics covered, and the depth to which they are covered, vary greatly; thus, students who graduate from different cybersecurity programs may have very different skills and abilities. And as these programs are introduced, what to cover and to what depth it should be covered are among the primary considerations in the development of the curriculum.

There is no universally agreed upon cybersecurity curriculum, and indeed there cannot be. The security needs of a military organization, a commercial firm, a hospital, and an academic institution are often distinct. For example, a commercial firm may prize integrity above other security properties to ensure its products are not tampered with as they are developed and go to market. A military organization treats confidentiality and integrity as the most important properties, as it must protect plans and disposition of troops and ensure only authorized changes by authorized people occur. A hospital must protect both, because a failure in integrity could result in the death of a patient, and a violation of confidentiality could result in a large fine and multiple lawsuits. Thus, no one curriculum can encompass all cybersecurity needs. So rather than a standard curriculum, a set of guidelines will enable institutions introducing new cybersecurity programs to select those areas of cybersecurity most relevant to the needs of their constituents (such as typical employers of their students), and emphasize those while covering the other topics in less depth. Institutions with existing programs can also use guidelines to determine whether their curriculum covers the material appropriate for their needs, as different cybersecurity curricula will emphasize different aspects of security.

The effectiveness of guidelines has been shown by the impact of the Software Engineering Body of Knowledge's (Bourque & Fairley, 2014) effect on software engineering education (Ludi & Collofello, 2001; Fairley, Bourque, & Keppler, 2014; Alarifi, Zarour, Alomar, Alkshaikh, & Alsaleh, 2016). It has changed how software engineering programs are developed and evaluated.

In September 2015, the Association for Computing Machinery (ACM) Education Board, the IEEE Computer Society, the Association for Information Systems Special Interest Group on Information Security and Privacy, and the International Federation for Information Processing's Technical Committee on Information Security Education collaborated to launch the CSEC2017 Joint Task Force on Cybersecurity Education (JTF).

For 28 months, the JTF engaged with the cybersecurity community through presentations and discussions at U.S. and international conferences and workshops. Members of an Industrial Advisory Board ensured that the resulting work included input from industries; members of a Global Advisory Board provided input from educators and professionals from around the world. In all, more than 325 people from 35 countries and 6 continents contributed to the development of the cybersecurity guidelines.

The first version of the Cybersecurity Curricular Guidelines (CSEC2017) (Joint Task Force on Cybersecurity Education, 2017) was completed in December 2017. This chapter discusses those guidelines, their use, and their future.

BACKGROUND

Before 2000, cybersecurity was generally considered of little interest in most, but not all, academic institutions. During the first decade of the 21st century, interest in cybersecurity as an academic area of