Cybersecurity Curriculum Framework

Jennifer Peyrot, Mark Emry, Dr. Jenny Daugherty, Dr. Melissa Dark, Dr. Dan Massey
University of Colorado, Boulder

Introduction

- As high school teachers integrate cybersecurity they need a coherent curriculum framework.
- A curriculum framework sets the parameters, directions and standards for curriculum policy and practice.
- It also enables educators to effectively plan properly sequenced activities so as to provide learning opportunities targeting desired learning outcomes.
- The framework used for Introduction to Cybersecurity was modeled after the AP Computer Science Principles curriculum framework, which is based on the Understanding by Design® (Wiggins and McTighe) model.
- Input was provided by educators from high school and higher education teaching in the computer science or cybersecurity courses.

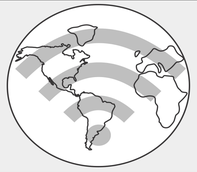
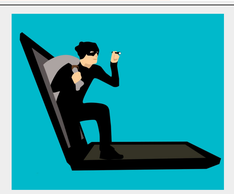
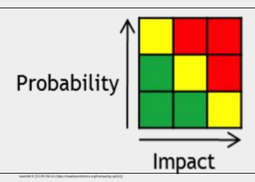
Related Work

Several resources that were referenced became a starting point for this work and are as follows:

- K-12 Computer Science Framework
- ACM CS Curricula 2013
- ACM IT Curricula 2017
- NICERC Framework
- NICE Cybersecurity Workforce Framework
- Code HS Curriculum
- PLTW Curriculum
- 2 Textbooks: Stallings & Brown and Bishop
- NIST Standards
- CAE - Knowledge Units
- Cybersecurity Curricular Guidelines - CSEC 2017

None of the resources provided a framework for a high school cybersecurity course.

Eight Big Ideas

Ethics - In this course, students will have the opportunity to evaluate the ethical implications among all stakeholders.	
Establishing Trust - Students in this course evaluate fundamental principles of cybersecurity and apply them to systems creating trust within organizations.	
Ubiquitous Connectivity - The more dependent we become on ubiquitous connectivity, the greater the implications if the network becomes compromised.	
Data Security - Students will study relevant laws and policies governing data; evaluate the tools used to connect cyber-physical systems; and practice using the encryption techniques needed to secure data across networks.	
System Security - System security introduces students to some specific vulnerabilities, and addresses the consequences of less secure hardware and software.	
Adversarial Thinking - Students in this course will challenge assumptions and practice thinking about opposing forces, in terms of intentions (when opposing forces are human adversaries), capabilities, and actions.	
Risk - This big idea engages students in this course with the risk assessment process as a methodology for grasping cybersecurity risk.	
Implications - Students in this course describe historical events and their cybersecurity implications examining the evolution of the threat environment at the local and global level.	

Preliminary Results

The CCF is posted on the Cyber Center for Education and Innovation (CCEI) website and requires interested parties to create an account prior to seeing the framework. This has allowed us to see who is interested in this work. As of the middle of October 2019, fifty people requested access. Two school districts, one in Alabama and one in Colorado, have started developing high school and middle school courses utilizing the framework.

Current Work

- Currently working with targeted educators to vet the curriculum in order to measure how well it can be used in the classroom.
- To see the CCF go to bit.ly/cyberframework or scan the code below:

Acknowledgements

Funding for the CCF comes from the Cyber Center for Education and Innovation (CCEI), a partnership between the National Cryptologic Museum Foundation and the National Security Agency.