Idea Submission

In order to address the shortage of a future cybersecurity workforce shortage, our efforts need to be focused on addressing the broader issue of technology education among our students. While children and young adults are presented with a multitude of electronic devices at home and in the classroom, the understanding of ‘how’ these devices work is lost. Without an understanding of ‘how’, how can we expect there to be understanding of the complex interactions and interdependencies within cybersecurity?

A video on YouTube, “Teens React to 90s Internet” with over 16 million views¹, depicts young adults experiencing an educational video about the Internet. They were asked questions about the meaning behind “.com” and “.org”, and “How do you get on the Internet?” The young adults simply do not know how the Internet exists but simply that it is “just there.” In addition to the problem of young adults not being taught, is the lack of technology teachers and curriculum to address the subjects.

I am proposing a mix of technical and non-technical topics discussed as part of every grade from elementary through high-school that advances in understanding and application as students progress. Younger grades are introduced to appropriate behavior, anti-bullying as part of activities that teach children right versus wrong; middle grades are focused on the parts and pieces that make up computers and the Internet, their functions and interdependencies; senior grades focus on theory, law, psychology and advanced certification studies.

Elementary / Grades 1-5

- Introduction to technology and appropriate behavior
- Game design through basic coding
- Cyberbullying

Middle school / Grades 6-8:

- Introduction to computer parts and pieces

¹Teens React To 90s Internet, Published 01 June 2014 by REACT https://youtu.be/d0mg9DxvfZE
• Design theory through hardware deconstruction
• Technical drawing and network design

High-school / Grades 9-12:

• Combining the human element and technical function.
• Educating on landmark technical cases involving privacy (FBI Stingray), Computer Fraud and Abuse Act (CFAA)
• Historical figures (Alan Turing, Vint Cerf, Grace Hopper) and their contributions to computers and the Internet
• Workforce needs and education/certification requirements

In my work with high-school and college interns is the idea that “it’s too hard” or, “it’s not relevant to me” would consistently arise. Having been presented with topics such as the privacy control settings for popular smart phone apps, understanding what data types are generated from their interactions online and the value of that data, and even providing demos of hacks used via Wi-Fi, lead them to become more engaged on the subject and understanding that it does affect them and their everyday actions. Additionally, that the material was not difficult, only that they had yet to be presented with the information in a manner that was consistent with how they digest it (both visually through delivery and writing style).

While this level of interaction may not be possible to all students, I recommend a partnership with organizations that can provide the tools and resources to our education system. ISC² provides cyberbullying education directly with students, Palo Alto provides cybersecurity education to young girls through Girls Scouts while Disney, Khan Academy, and Tynker (among others) support ‘Hour of Code’ programs.

These programs are provided freely by both non-profit and commercial companies as part of a broader understanding of the need to teach our students these valuable skills. I propose requiring a larger commitment from commercial, non-profit and academia to provide education and training classes to high school students on cybersecurity. As students prepare to join the workforce, each individual is responsible for practicing ‘good cyber hygiene’ and it is within
these organization’s best interests to ensure the next workforce understands their role and responsibilities to their employer regardless of their job title. It is also within these organization’s best interest to interact with students on ethics, intellectual property, data breaches, risk management and consumer protections and privacy.
BIO

Michelle Duquette is a cybersecurity advisor supporting Government clients and Fortune 500 companies for over 10 years. Michelle has worked with integrated product teams and advised senior leaders on the issues of security engineering, Cybersecurity policy management, and information risk management across varying government classification levels. Michelle works as a Cyber Security Advisor with Battelle Memorial Institute and previously as a Senior Consultant for Booz Allen Hamilton, and a Software Engineer with Lockheed Martin.