Contact: Michelle Duquette duquettem@battelle.org

Cybersecurity Education for All Education Levels

In order to address the shortage of a future cybersecurity workforce, 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 this understanding, 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 views[1], 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, only 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 these subjects.

I propose a mix of technical and non-technical topic discussions as part of every grade from elementary through high-school that advance in understanding and application as students progress. Younger grades are introduced to appropriate behavior, e.g. 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

- Code design using toys

- Cyberbullying

Middle school / Grades 6-8:

- Introduction to computer parts and pieces

- Coding and game design

- Design theory through hardware deconstruction

- Technical drawing

- Internet- design and theory on how it works

High-school / Grades 9-12:

- Advanced topics in network design, coding, reverse engineering, algorithms

---

[1] *Teens React To 90s Internet*, Published 01 June 2014 by REACT https://youtu.be/d0mg9DxvfZE

- Combining the human element and technical function

- Educating on landmark technical cases involving privacy (FBI Stingray), Computer Fraud and Abuse Act (CFAA)

- Historical figures (e.g. Alan Turing, Vint Cerf, Rear Admiral Grace Hopper) and scientific developments (e.g. ENIAC, DARPA) for their contributions to computers and the Internet; Bletchley Park, Becky Base, Diffie-Hellman, RSA for their contributions to computer security

- Workforce needs and education/certification requirements in conjunction with the NICE Cybersecurity Workforce Framework

In my work with high school and college interns, the idea that "it's too hard" or, "it's not relevant to me" would consistently arise. Conversely, teens and young adults 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 build their understanding that cybersecurity does affect them and their everyday actions. This lack of understanding on how technology and devices work lead model Karlie Kloss to work with Teach for America to reach 25 cities with 50 coding camps within 3 years. Ms. Kloss cites that her public high school did not offer computer classes but understands the growing need for coding education and has communicated this need to her 12+ million social media followers.[2]

While this level of interaction may not be possible with all students, I recommend a partnership with organizations that can provide the tools and resources to supplement our education system. For content aimed at elementary and middle school grades, ISC[2] provides educator kits for teaching online safety to children covering privacy, safe posting and cyberbullying[3], while Disney, Khan Academy, and Tynker (among others) support 'Hour of Code' programs. Additionally, *CyberStart*, a suite of tools and games designed to introduce children and young adults to the field of cybersecurity developed by the SANS Institute could be used to teach younger children the application of relevant security topics.[4] For content aimed at high-school students, Cybrary offers a mix of free content ranging in technical to higher-level security management concepts, and the for-profit company, EC-Council, offers a certificate course, Certified Secure Computer User, "aimed at today's computer user to learn how to safely browse, watch videos, send email and work online".[5] Arguably, the content has been created, is reasonably available, and is ready for consumption and integration with course curriculum.

---

[2] *Model Karlie Kloss Sees Big Growth For Her Coding Camp for Teen Girls,* Published March 16, 2018 by Forbes. https://www.forbes.com/sites/susanadams/2018/03/16/model-karlie-kloss-sees-big-growth-for-her-coding-camp-for-teen-girls/#5b45889578d3
[3] Safe and Secure Online *Educator Kits and 1:1 Learning*; https://safeandsecureonline.org/educators-and-leaders/
[4] SANS *CyberStart*, https://www.sans.org/cyberstart
[5] EC-Council, *Certified Secure Computer User (CSCU) Course*, https://iclass.eccouncil.org/our-courses/certified-secure-computer-user-cscu/#1493241110424-4ca4541e-0aec

Contact: Michelle Duquette duquettem@battelle.org

These programs are provided 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 its role and responsibilities to its employers regardless of job title. It is also within these organizations' best interest to interact with and educate students on ethics, intellectual property, data breaches, risk management and consumer protections and privacy.

Contact: Michelle Duquette duquettem@battelle.org

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.

Michelle holds both a M.S. in Computer Science and a Graduate Certificate in Information Assurance and Cybersecurity from George Washington University, and a B.S. in Information Management and Technology from Syracuse University. Michelle is a Certified Information Systems Security Professional (CISSP) and Certified Ethical Hacker (CEH). Michelle presented at the 2015 American Petroleum Institute 10th Annual Cybersecurity Conference on, "Biometrics: What is it and Where Do I Begin?"; published internationally in the July 2014 Information Systems Security Association Journal, "Our Children's Future: As Determined by Their Online Identity", and on the panel for TechWeekDC 2017 for 'Women Take on Careers in Tech' providing insight on how to start a career within cybersecurity in DC, perspective on how to create the career you want, and personal experiences.