Integrating Cybersecurity into the K-12 Classroom

We are living in the midst of a social crisis as technology rapidly expands and bad actors take advantage of our democratic system. America's belief in the power of liberty and open systems comes with drawbacks such as opposition to preemptive, offensive, or aggressive actions taken in the field of cybersecurity by our own government officials. Achieving the balance between liberty(privacy) and security is a challenge. As a country we should strive to "future" proof the education provided in cybersecurity. To achieve this worthy goal an emphasis on teacher development and an intentional expansion of resources into the K-12 environment must occur. A job shortage of a predicted 1.8 million people by 2022 (CSO Online, 2015) and the increased need to teach digital natives basic cybersecurity survival skills, (Irish Times, 2018) require that cybersecurity be integrated in a multidisciplinary fashion in the K-12 classroom. Educating the populace in the field of cybersecurity is necessary for three concrete reasons: 1. To prepare students for an ever-increasing technology-based future; 2. To expose students to the jobs and careers available in cybersecurity; 3. To defend our nation from the many types of cyberwarfare tactics performed by America's adversaries. This initiative can best be started in the K-12 system.

Multiple stakeholders must be involved in order to develop the most impactful, institutionalized design possible; a design that impacts the most students while still allowing the individual classroom teacher freedom to be creative and adaptive. If this crisis is left solely to politicians, it may fail.

The following model is presented for discussion, debate, and open dialogue:

a. Establish regional teacher learning communities, sometimes referred to as professional learning communities. This is a recognized best practice that can both enhance teacher quality as well as empower teachers to lead. Teacher quality is the single most important factor when determining student success in the classroom. A teacher learning community (TLC) is not a staff meeting. Instead, a TLC focuses on collaboration, continuous improvement, and a growth mindset in

CSO Online: http://www.csoonline.com/article/2953258/it-careers/cybersecurity-jobmarket-figures-2015-to-2019-indicate-severe-workforce-shortage.html
Irish Times Online: https://www.irishtimes.com/news/education/the-myth-of-digital-natives-1.3459381

order to both teach the educator new skills as well as allow a place for dialogue. Within a TLC, teachers can share strategies and lessons that work as well as share items that do not work. This teacher-centered approach improves educator awareness and quality in order to benefit student learning. These TLCs also could create ideas for incorporating a standard based, multidisciplinary cybersecurity curriculum throughout the United States.

b. In order to be impactful, these TLCs will need a relationship with post-secondary academia and local cybersecurity experts. It is suggested that each TLC be led by at least one master teacher in each region. This master teacher would serve as a link between higher education, government/industry, and the K-12 environment as well as be responsible for leading established monthly professional development sessions on cybersecurity topics. The master teacher would need basic cybersecurity knowledge and serve to help others learn and adapt for individual disciplines.
c. All teachers will also need access to a shared online database or website to share and explore lesson plans. This website would allow interested teachers a "one stop shop" to explore lesson plans and activities for the K-12 classroom. Teachers would also be encouraged to adapt posted lessons and/or share new lesson plans to create the best resource possible. Contained within this website will be a cyber-ethics module for students in each grade band (grades 3-5; 6-8; 9-12). This ethics module could be used by all disciplines and all teachers in the K-12 classroom to instill necessary ethical guidelines.
d. After the establishment of the TLCs, a grant program could be established to bring longevity and a local approach to teaching cybersecurity within each school district. Under this proposal, interested school districts could apply for grant money to fund one cyber literacy outreach coordinator for the district. Responsibilities of this individual would mirror the established practice of utilizing instructional coaches within the K-12 setting. The cyber literacy outreach coordinator would "coach" individual classroom teachers in lesson development, hands-on activities, and co-teaching opportunities to both create new lessons and implement cybersecurity topics into current lessons. This person would also be responsible for attending professional development opportunities such as the

NICE K-12 conference to stay current and up to date on cybersecurity trends. The instructional coaching model has proven to be effective. Instructional coaches help teachers become better teachers by facilitating creativity and best practices. Better teaching methodology leads to higher student production.

e. Continuous in-person professional development should occur in the form of one-day cybersecurity boot camps that use the "teach the teacher" model. These events could occur in each region to begin the process of institutionalizing cybersecurity concepts into the classroom. The one-day boot camps would advertise to all teachers regardless of discipline or experience. A beginner session; along with an advanced session would be offered. Not only is there a desire amongst teachers who lack experience, but experienced technology/CS teachers strongly desire guidance in implementing cybersecurity into their coursework. Some teachers may not have the time or desire to commit to a TLC. However, completing a one-day session may encourage them to join the community.

The strategies described in this document are already being used; only the content topic has changed. Placing an increased emphasis on funding cybersecurity education initiatives in K-12, utilizing proven teacher development strategies, and establishing a community of multidisciplinary cybersecurity advocates within the K-12 setting will institutionalize the process of educating students on cybersecurity at a young age. These actions will solve the job shortage crisis, make Americans better cyber citizens, and prepare the nation for the ongoing struggles with foreign adversaries and bad actors.

Biography

Ms. Ashley Greeley received both her Bachelor's and Master's degrees from Purdue University. She began her teaching career in 2003. After two years in the special needs classroom, Ms. Greeley began teaching social studies at Harrison High School (West Lafayette, IN). While at Harrison, she developed two new courses for insertion into the curriculum (AP US history and AP US government), coached a variety of sports and an academic team, served as both department and corporation chair, led the school improvement team, facilitated teacher professional development, and served in whatever capacity asked of her. Greeley was awarded numerous teaching awards and recognition including the Golden Apple, the DAR History Teacher of the Year, the Indiana Historical Society Teacher of the Year, the Indiana History Teacher of the Year, the Indiana representative at the Supreme Court Summer Institute, and was a top-25 finalist for the Indiana Teacher of the Year Award. Beginning in 2015, Greeley began serving as a site visitor for GenCyber summer camps. In 2017, Ms. Greeley was awarded an NSA/CAE grant to develop a multidisciplinary K-12 cybersecurity curriculum as well as perform cybersecurity outreach for Tippecanoe School Corporation as an extension of the INSuRE program at Purdue University.