Onramp to cybersecurity Labor Pipeline through K12 Classroom Education

Meg J Ray
Teacher in Residence
Cornell Tech

Tim Winston
Principal, PA-QSA(P2PE), CTGA, CISSP, CISA
Coalfire Systems

Key to solving labor supply issues in cybersecurity is a strategy that begins well before college. To achieve a diverse pipeline of cybersecurity professionals and a populace educated in basic data privacy and security concepts, we must build and fund a coherent K12 strategy that makes sense in our current school system and brings together the expertise of cybersecurity and education specialists.

The primary need is a future-proof and readily available labor pipeline in the US. The impact of Moore's Law on all current technology spaces (ie. mobile devices, cloud computing, IOT) not only applies to increasing computational power but more generally to the exponential expansion of all types of capabilities. Given this circumstance, future proofing our workforce will not be about anticipating technological development, but about preparing professionals who can assimilate new technologies quickly, apply foundational concepts in novel situations, and are fluent in metacognitive skills. Although students will still require areas of technical proficiency, this mindset requires a shift in our approach to education. Students will still need to develop one or two areas of technical proficiency. This will allow incoming professionals to fully appreciate how to secure and apply cybersecurity principles, to one area that they understand deeply before generalizing to a wide range of technologies.

Technical roles are not the only need to be addressed in cybersecurity labor supply. The technically oriented attacker and defender roles may be the first and only ones that come to mind, but there are many others on a team that are vital to supporting these roles. In the cybersecurity field we also need skilled project managers, educators, designers, and grant managers. People who do not have the interest or opportunity to pursue the engineering side, need to know that there are still critical careers in cyber security where they can make a crucial contribution.

A secondary need that K12 education can address is a cybersecurity literate population. This type of general literacy can only help the efforts of cybersecurity specialists on a broad scale. A better understanding of security and privacy is more important than ever: policy makers at all levels, developers and data scientists, CEOs and CFOs in all industries, and voters. It is of vital importance that individuals across industries understand the value of, and threat to, their personal and professional data. In this way individuals would better understand and support the need to properly protect information.

We can lift important lessons from recent efforts to broaden access and awareness in STEM and CS education. Early positive math and science experiences and career awareness, especially at the middle school level, is important to recruiting interest particularly for underrepresented student populations (Maltese & Tai, 2011; Moakler & Kim, 2014). Leaving relevant classes and experiences only to those who opt in, excludes large numbers of talented students. Barriers include issues of student identity and obstacles to access, such as needing to hold an after school job or attending a school that does not offer AP classes (Margolis, 2008; Wang & Degol, 2013). To address these needs, we propose a multi-pronged approach touching all levels of K12 education.

First, all children need a basic understanding of how the digital world works. As outlined in the K12 CS Framework, they should understand the basics of computers, networks, and data. In order to recruit interest in cybersecurity and prepare students for required classes, it is important that they do not leave high school with the vague idea that it works “somehow” or by “magic.” Children's innate temptation to misuse things can actually be a positive indicator for both STEM and specifically security. Rather than simply correct the impulse - it can identify the aptitude and redirected to the importance of building and testing securely. These concepts can be fit into CS, technology, or science classes. Elementary school students are introduced to these concepts through the use of stories and physical activities that model computing processes. As students move up, they are able to learn lower level concepts and incorporate them into projects that reflect real world contexts.

In middle school, many schools begin to teach digital citizenship. There is a tendency in CS education to draw a hard line between technology/digital citizenship and computer

science/coding. We need to soften this line and reboot our middle school curriculum. Digital citizenship education 2.0 must involve more than anti-cyberbullying campaigns. Students should learn web safety as well as web development. They learn to not give their personal data to strangers, but should also learn how their data is tracked with routine web use and how to secure and protect their own data.

In high school, it is appropriate for all students to learn and think about the current and historical context of cybersecurity. In social studies classes, units should be supplemented to include themes related to surveillance, privacy, protecting our capabilities, ethics, etc. They should understand personal and national security as themes in wartime and peacetime and how historical events have impacted current issues.

In high school, we can broaden current CS learning for students who are taking higher level math and CS courses to prepare for STEM careers. CS classes need to incorporate opportunities for students to have counter functional experiences, by “breaking” each other's work and by finding new use cases. This “make it, then break it” approach also addresses practices and metacognitive skills in the K12 CS Framework that are more difficult to teach. For example, we want students to understand that projects are never just done. There are always iterations that can be made based on need and context. We also want students to know that making something work technically is just as important as developing soft skills like problem solving, self-reflection, and project management. We can open the doors of CS experiences such as robotics clubs and engineering classes to a wider group of students by explicitly creating and valuing roles project manager or publicist.

In order to make this K12 strategy a reality, two areas need to be addressed. First, we need quality curriculum disseminated effectively to teachers. This type of curriculum is best developed within partnerships between education and cybersecurity experts. Disseminating curriculum means building partnerships with trusted education websites across disciplines. Teachers cannot teach curriculum that they do not know about. Second, we need to train teachers. Unfortunately, cybersecurity is an area about which many lay people hold misconceptions. Looking again to recent developments in CS education, we know that professional development is a complex problem to address due to issues of scale, fidelity, and

teacher interest and capacity (Pollock, et al., 2017). However, a blend of online and in-person training as well as partnerships with school districts, non-profits, industry, and universities, makes it possible. The approach we have outlined is built for minimal change in the school day and is a relatively light lift, based on doable changes such as supplementing lessons or units in existing curriculum. If stakeholders in K12 education, universities, and industry work together, it is possible to create an effective primary and secondary education strategy that will be the cornerstone of cybersecurity literacy in the general population and play a key role in increasing and diversifying the cybersecurity labor pipeline in our country.

BIO SKETCH

Tim Winston | PA-QSA(P2PE), CTGA, CISSP, CISA | Principal
Tim Winston is a Principal Consultant in Point-to-Point Encryption (P2PE) and encryption key management at Coalfire Systems. Tim is an information security and risk professional with over 35 years of experience in all aspects of information technology. He has extensive experience in software development, networking, access control systems, identity management, cloud platforms, and has provided cyber security expertise to the largest cloud platform providers, payment terminal manufacturers, encryption service providers, payment service providers, government agencies, biomedical research organizations, healthcare solution providers, critical infrastructure providers, e-commerce service providers, and retailers.

Meg J Ray
Meg Ray is the Teacher in Residence at Cornell Tech. Meg is responsible for the implementation and design of the Teacher in Residence program, a coaching program for K-8 CS teachers in New York City schools. Meg served as a writer for the Computer Science Teachers Association K-12 CS Standards and as a special advisor to the K12 CS Framework. She is an experienced high school computer science teacher and special educator, and also taught graduate-level education courses at Hunter College. Previously, Meg directed the design of a middle school CS curricula. She researches CS teacher training as well as access to CS instruction for students with disabilities. Her work is published in academic journals and conference proceedings. She has a forthcoming intro to programming book aimed at middle and high school students. Meg holds a Master's of Science in Special Education from Hunter College and a Graduate Certificate in Blended Learning and Computer Science Instruction from Pace University.

CITATIONS

K–12 Computer Science Framework (2016). Retrieved from http://www.k12cs.org.

Maltese, A. V., & Tai, R. H. (2011). Pipeline persistence: Examining the association of educational experiences with earned degrees in STEM among U.S. students. Science Education,95(5), 877-907. doi:10.1002/sce.20441

Margolis, Jane. (2008). Stuck in the shallow end : education, race, and computing. Cambridge, Mass. :MIT Press.

Moakler, M. W., & Kim, M. M. (2014). College Major Choice in STEM: Revisiting Confidence and Demographic Factors. The Career Development Quarterly,62(2), 128-142. doi:10.1002/j.2161-0045.2014.00075.x

Pollock, L., Mouza, C., Czik, A., Little, A., Coffey, D., & Buttram, J. (2017). From Professional Development to the Classroom. Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education - SIGCSE 17. doi:10.1145/3017680.3017739

Wang, M., & Degol, J. (2013). Motivational pathways to STEM career choices: Using expectancy–value perspective to understand individual and gender differences in STEM fields. Developmental Review,33(4), 304-340. doi:10.1016/j.dr.2013.08.001