CERIAS Tech Report 2024-6 Impact Report: Robust Cybersecurity Education by Melissa Dark, Jenny Daugherty, Sabrina Smiley, Nancy Stevens

Center for Education and Research Information Assurance and Security Purdue University, West Lafayette, IN 47907-2086



Impact Report

DARK Enterprises, Inc



Contents

1 Introduction - A message from the Founder

2 Vision, Mission, Values

3

What is foundational knowledge in cybersecurity education?

4

What is the status of cybersecurity education in secondary schools?

5-6

How can we support robust cybersecurity education?

7

Board of Directors and Team



This report describes the work of DARK Enterprises following the management of the GenCyber program for 7 years. What we've accomplished was shaped by those formative years. The change we have been able to create so far is rewarding. I am grateful to the staff who were integral to this work - Dr. Jenny Daugherty, Nancy Stevens, and Sabrina Smiley - the Board of Directors, our partner organizations, and our funders.

DARK Enterprises, Inc was founded in 2015 to house a single grant that infused cybersecurity into the high school AP Computer Science Principles course. In less than a year, I was asked to help the National Security Agency launch GenCyber, a new national out of school time program to build interest in cybersecurity among students and teachers in K-12 schools. Both GenCyber and the AP CSP project launched K-12 cybersecurity education in our Nation in the interest of building a robust and reliable cybersecurity talent pipeline. By 2017 we were seeing fledgling

"Whether it is the end of the day or the end of a project, we endeavor to do and to inspire good work."



cybersecurity courses in schools, and teachers were asking questions such as "What should I teach", and "Where do I find curriculum?" During my time at Purdue University, I'd heard and been a part of answering the same questions in the post-secondary education community. In 2019, I decided to use my experience growing cybersecurity education in U.S. colleges and universities to steward growth of cybersecurity education in U.S. K-12 schools full-time. This was the second beginning for DARK Enterprises.

K-12 Cybersecurity Education is at an interesting juncture in the U.S.: 1) we have nearly 10 years of experience in K-12 cybersecurity education, 2) our Nation still has a cybersecurity workforce shortage, 3) cybersecurity is a fast-moving field, and 4) other nations, including our adversaries, have strong cybersecurity talent pools. So there is more work ahead. I look forward to support and partnerships in this good work.

Sincerely,

Milian Dark



Our vision:

DARK Enterprises, Inc a 501(c)(3) is dedicated to assuring the U.S. has a robust and reliable talent pipeline in cybersecurity.

Our mission:

To realize this vision, we provide leadership, resources, training, and partnerships to develop excellent cybersecurity education at the secondary level.

Our values:

We value good stewardship. Our approach is to formulate relevant questions, collect and analyze data, partner, and effectively communicate results. This impact report shares our achievements from 2019-2024 in pursuit of the following questions:

- 1. What is foundational knowledge in cybersecurity education?
- 2. What is the status of cybersecurity education in secondary schools?
- 3. How can we support robust cybersecurity education?





Foundational knowledge in any discipline is the basis for more advanced learning. And the foundation can shift as the discipline evolves. We have prioritized this question because cybersecurity is a new discipline, therefore, developing a robust, shared understanding of the foundation helps build a strong community.

The High School Cybersecurity Curriculum Guidelines (HSCCG) established the first framework in the U.S. for a high school cybersecurity course. The HSCCG framework work found that the foundation of cybersecurity is 8 big ideas: Ethics, Trust, Data, Network, Systems, Risk, Adversarial Thinking and Implication. This collaborative effort involved educators in high school and higher education, as well as government and industry leaders with a need for highly skilled cybersecurity workers. Over the past five years, the HSCCG have been used as the basis for several cybersecurity curriculum projects now used across the U.S.: Teach Cyber, Regions Investing in the Next Generation (RING), the Army JROTC Cyber program, and UTeach Foundations of Cybersecurity.



You can't build a great building on a weak foundation.

As the HSCCG has gained recognition, we sought to move the work to a professional association known for curating internationally accepted curriculum guidance, i.e., the Association for Computing Machinery (ACM). In partnership with university, community college and high school faculty, the HSCCG is being reinvented as a supplement to CSEC 2017, the ACM Cybersecurity Curricular Guidelines used by ABET to accredit collegiate cybersecurity programs. Our update describes what schools should teach in a foundational cybersecurity course, what some might call Cyber 1. The audiences for this work include secondary and post-secondary schools with the intention of enabling the growth of early college credit in cybersecurity.

Technological advancements will continue to change what is considered foundational knowledge. The current discussions regarding artificial intelligence and how it impacts knowledge and skills of the workforce is just one example. We continue to engage with partners willing to explore this question of foundational knowledge. Given our mission to develop excellent cybersecurity education at the secondary level in the U.S., we seek to understand not just where we are going, but where we are today.

CyberSupply is empirical research on the availability of cybersecurity courses in schools and access to students. It is the only source of such data in the U.S. With limited funds, we used representative sampling to analyze availability of and access to high school cybersecurity in rural vs suburban schools, in low SES vs high SES schools, and in schools with majority White vs. majority STEM underrepresented student populations. To date, the work has been a partnership with the National Cryptologic Foundation, Murray State University and the University of Arizona. The CyberSupply research, analysis, and summary reports are being used by stakeholders across the represented states as well as the College Board in

> In the gap between where we are and where we want to be lies our greatest opportunity for growth.



their advocacy for cybersecurity. We are open to new partnerships and opportunities to expand this work.

Our research also finds that high school cybersecurity is typically a single course in an IT pathway. While some states position a cybersecurity course in a computer science or STEM pathway, the dominant trend of placing cybersecurity in an IT pathway limits it to networking and network security. We strive to inform and promote a more all-encompassing view of the field. The ACM CSEC 2017 update outlines six knowledge areas in a foundational cybersecurity course: data security, network security, system security, software security, organizational security and societal security.





The last question that guides our work falls out of the first two. If we aim for developing excellence in cybersecurity in U.S. schools, and we understand the gap, then how do we go about closing the gap?

Teach Cyber is a library of 46 cybersecurity curriculum lessons covering foundational cybersecurity per the High School Cybersecurity Curriculum Guidelines. Teach Cyber was built to support teacher adoption and student learning in three ways: 1) it is available to teachers in the U.S. at no cost, 2) it can be implemented in a complete course or adapted to work with another curriculum, and 3) it builds student interest and engagement through active learning. Our partnership with The National Cryptologic Foundation (NCF) enabled this work. In 2024 our newest partner, UTeach at the University of Texas in Austin, launched a derivative of Teach Cyber. This update is a full year-long cybersecurity course using the Codio learning platform and provides teaching resources in a single place with a full menu of teacher support options.

The Assessment Resources in Cybersecurity (ARC) project implements the HSCCG into assessment thereby giving teachers the full suite of guidelines, curriculum, and assessment. This project provides two key resources: a bank of assessment items that teachers can use and guidelines for teachers to write additional items beyond what is available in the item bank. A priority for DARK Enterprises has been highly qualified cybersecurity teachers in America's high schools. Toward this end, we offer a range of teacher professional development programs: online teacher professional development to support teachers using Teach Cyber., 2) professional development for Wyoming teachers (in partnership with the Wisconsin Cooperative Educational Service Agency, 3) an asynchronous open enrollment course on Foundations of Cybersecurity, and 4) an 18 credit hour graduate certificate. The OER course and the graduate certificate are offered through the National Cybersecurity Teaching Academy (NCTA), which is a partnership with 8 universities, NCTA is the biggest teacher professional development program we have launched and is the first and only program building deep content knowledge in cybersecurity. With grant support, NCTA provides scholarships to support qualified teachers the graduate certificate, which positions teachers in many states to teach dual credit foundational cybersecurity.



The shortest distance between two points is a straight line.

d's Anolino

West 3

6

In addition to building capacity in secondary cybersecurity education, our work focuses on building bridges from high school to college cybersecurity education. Our work on Early College Credit in Cybersecurity (E3C) examines the viability of this strategy for increasing collegiate cybersecurity study and building the cybersecurity workforce. To date our work has examined models of E3C as exemplars, and investigated the potential for scalability and ROI. We expect the E3C work to begin a new phase of implementation as we roll out a model Cybersecurity Foundations course to NCTA alumnae aligned to the CSEC 2017 promoting dual credit opportunities at NCTA universities.

Lastly, we support cybersecurity education by serving as external evaluation experts. We have conducted small to large scale program evaluation for NSA's GenCyber Program, Cyber Florida's Cyber/IT Pathways Grant Program and with SAIC/Army JROTC Cybersecurity. The Teach Cyber website is the portal to the resources we provide to the cybersecurity education community. These resources include the HSCCG, teaching modules, ARC assessment guides and itembanks, CyberSupply infographics, and early college credit information.

	Website Numbers
Teach Cyber website	1794 subscribers
Unit 1 Teach Cyber	1189 downloads
TC Glossary	255 downloads
TC Club Kit	922 downloads
US Cyber Range Lab Files	1648 downloads
CyberSupply infographics	712 downloads
CyberSupply website	5742 site visits
E3C Report	44 downloads
US Cyber Range Support	
Range access grants	1600 students & teachers
NCTA	
NCTA graduates	83
NCTA enrollment	160
New NCTA scholarships	350





Dennis Depew, PhD

7

Dennis serves as Dean Emeritus and Professor of Engineering and Engineering Technology in the College of Business and Technology at ETSU.

He also served as Dean of the College of Technology at Purdue University from 2002-2011, and as Dean of the College of Applied Sciences at Western Carolina University from 1999-2002.

Vera Zdravkovich, PhD

Vera has worked with DHS, NSA, and NSF to establish the Center of Academic Excellence Two-Year designation that came to fruition in 2010. She led the national project while working with community colleges nationally to support their cybersecurity programs.

She has served on diverse state and national committees for science and technology education.

Nate Evans, PhD

Nate is a senior cybersecurity researcher at Oak Ridge National Laboratory. He works on a variety of proactive cybersecurity projects involving critical infrastructure.

He created a cybersecurity assessment for critical infrastructure that is used by DHS. He has earned three R&D 100 Awards for his research in proactive cybersecurity.

Team



Melissa Dark



Jenny Daugherty



Sabrina Smiley



Nancy Stevens







DARK Enterprises, Inc

