Editors: Jens Grossklags, jens.grossklags@in.tum.de | Jelena Mirkovic, mirkovic@isi.edu | Bill Newhouse, newhouse@nist.gov

Designing a K–16 Cybersecurity Collaborative: CIPHER

Karen L. Sanzo, Jay Paredes Scribner, and Hongyi Wu | Old Dominion University

Cyberattacks have become more common, sophisticated, and harmful, while, at the same time, there is a critical shortage of cybersecurity professionals. For example, from October 2019 to September 2020, there were more than 40,000 unfilled positions for information security analysts.[2] While educational organizations have responded to this burgeoning demand, cybersecurity education and training institutions in the United States have found it difficult to keep pace with the growing call for cybertalent.

Three significant challenges—untapped pools of talent, a lack of diversity in the field of cybersecurity, and inadequate standardization within and across K–16 institutions—impede the identification and cultivation of quality cybersecurity professionals. Although many universities have established cybersecurity degrees, concentrations, and certificate programs, a significant gap exists between K–12 and college education in cybersecurity.[6] It also remains deeply challenging to achieve diversity and inclusion in the cybersecurity field. Additionally, there are no standardized articulations regarding cybersecurity between elementary schools, middle schools, high schools, community colleges, and four-year universities, and there is no guarantee that students at the same grade level are introduced to identical academic content and skills.[3,5]

In this article, we share initial findings from the testing of a proposed framework to address the aforementioned challenges in establishing a K–16 pipeline to prepare cybersecurity professionals. The goal of the initiative is to create a researcher–practitioner partnership (RPP) that paves the way for a national alliance for the development of fundamental, theoretically grounded, and systematic approaches to inclusive K–16 cybersecurity education, especially for students who have a low socioeconomic status (SES). The Cybersecurity Inclusive Pathways Toward Higher Education and Research (CIPHER) model brings together scholars from multiple disciplines and practitioners from various fields to collaborate and fully understand the problems explicated here and to coconstruct a K–16 partnership model to address those challenges.

The planning phase is designed to substantially shape the development of CIPHER. This process, using a design-based implementation research (DBIR) approach, enables us to iteratively test ideas with stakeholders, engage with partners to co-design and test evolutions of CIPHER, and develop a model that can be implemented and scaled up with fidelity.[4] Ultimately, this will lead to a clearly articulated vision and mission for the CIPHER alliance, a well-planned structure and guidelines, and clear road maps for research, education, outreach, and diversity.

DBIR

We use a DBIR approach, which is an extension of design-based research (DBR).[4] Hallmarks of DBR include tenets highlighted by Anderson and Shattuck:[1] being situated in a real educational context, focusing on the design and testing of a significant intervention, using mixed methods, involving multiple iterations, building a collaborative partnership between researchers and practitioners, evolving design principles, and making a practical impact. Further, DBIR extends DBR through a focus "on building organizational or system capacity for implementing, scaling, and sustaining educational innovations."[4] Through this research lens, we are

Digital Object Identifier 10.1109/MSEC.2021.3050246
Date of current version: 15 March 2021

 Copublished by the IEEE Computer and Reliability Societies

able to present our initial conception of CIPHER to partners and co-design the initiative with educators; make real-time, progressive changes to the model; have tangible and immediate impacts on practice; and study the efficacy of the work. We present the findings from our initial two DBR iterations of CIPHER, including results from our launch meeting and how the model has evolved based on partner collaboration. We conclude with anticipated next steps for the initiative. Readers are encouraged to contact us, in the spirit of DBIR, to provide feedback and if they would like to be part of CIPHER or begin a similar enterprise.

Iteration 1

The first iteration of CIPHER was developed based on stakeholder survey feedback and a four-hour meeting with more than 35 participants, drawing from K–12 school districts, state-level educational agencies, institutions of higher learning, and industry partners. The survey provided an overview of the purpose of CIPHER and was used to understand if the model resonated with potential partners, ask about who should be included in the planning, and discover initial impressions. These data were used as grounding for the CIPHER launch meeting with stakeholders. The purpose of that meeting was to further explore the model and the emerging vision, present the preliminary concept of having five "task forces" to aid in development, and solicit focus group input through four facilitated breakout groups. The task forces and their purposes are described in the following:

- *Administration and Articulation Task Force*: engage the CIPHER community, identify the leadership team, and develop a plan for coordinating K–16 schools and colleges to establish articulations across the years of schooling to define the pathways for cybersecurity education
- *Diversity Task Force*: develop plans for inspiring and improving the participation of underrepresented groups and low-SES students
- *Human Resource Development Task Force*: identify effective ways to support teachers, counselors, and administrators to integrate cybersecurity into content areas in K–12 curriculum
- *Infrastructure Task Force*: understand the structure support in different schools and classify schools into three tiers: those with high-SES students and substantial computer and Internet infrastructure (tier 1), those with computers for every student but limited Internet access (tier 2), and those with many low-SES students and no computer and Internet infrastructure (tier 3); make recommendations on curricula and infrastructure support to ensure the equity of the proposed cybersecurity education
- *Research and Assessment Task Force*: develop an assessment plan; identify a pilot program to test hypothetical approaches, collect data, and understand what administrators/teachers/counselors/parents need to know and be able to do to support cybersecurity education; create a plan to disseminate research outcomes and solidify CIPHER partnerships.

We asked numerous questions: What are your hopes and expectations for a cybersecurity collaborative? What are considerations we should be cognizant of moving forward? Looking ahead three to five years, what will success look like for CIPHER? What should our immediate next steps be? The following focus group themes aided in the development of the second iteration of CIPHER:

- *Creating a central hub*: Attendees expressed a desire to streamline myriad initiatives in the cybersecurity education space. The collaborative emphasis of CIPHER was seen as beneficial, as there was a lack of collaboration among school districts that had cyberinitiatives (generally due to a lack of capacity and funding resources); a central coalescing mechanism such as CIPHER could address that gap. Essentially, the attendees believed CIPHER was necessary and felt that the initiative's timing was serendipitous.
- *Collaborating, not "bombarding"*: Another interesting but not surprising finding was that K–12 faculty sometimes felt that higher education institutions were "bombarding" them with initiatives, although colleges and universities could also be seen as "partners" and "collaborators." The attendees viewed CIPHER as highly favorable due to the central role K–12 educators would have in the initiative.
- *Building an authentic pipeline*: Much of the conversation around this question revolved around

Cyberattacks have become more common, sophisticated, and harmful, while, at the same time, there is a critical shortage of cybersecurity professionals.

developing a collaborative "pipeline" from K–12 schools to higher education to the workforce. The need to focus on a comprehensive cybersecurity curriculum, access for all students, and training for teachers would be embedded in the concept. While there appeared to be pockets of success in crafting cybersecurity curricula and providing training to teachers, none of the attendees cited a cohesive framework/approach. Some school representatives said there were different departments within the same district that oversaw cybersecurity efforts but rarely interacted. For example, in one district, the responsibility for developing and teaching cybersecurity could be spread across the career and technical education, science, and mathematics departments, with little collaboration.

- *Partnering with employers*: Businesses expressed concern about the challenges to finding cybersecurity talent and the need to establish internships and apprenticeships for high-schoolers and university students. A centralizing hub, such as CIPHER, was seen as a viable mechanism to broker partnerships across educational and industry boundaries while engaging in substantive research to learn iteratively about how to better establish collaborations.
- *Taking action, not just meeting*: The attendees spoke to the need for immediate action and said they did not want to be involved in a years-long "planning-only" initiative. Attendees saw CIPHER's initial focus on planning and development as a drawback and expressed the need to demonstrate immediate, actionable results to prove the concept and build trust with partners. They advocated for small work groups with specific time frames and deliverables. As part of the action orientation, attendees affirmed the work group concept in the original CIPHER design
- *Fostering inclusivity*: Attendees described the need to include representatives from all stakeholder groups, including teachers, administrators, school counselors, business partners, higher-education personnel, and students.

Iteration 2

Changes were made to the CIPHER planning and to the initiative's mission and vision based on the survey data and focus group findings from iteration 1. We combined the Diversity and Infrastructure task forces into one group to eliminate redundancy. The task forces were populated with volunteers from the initial launch meeting and with additional educators recruited through monthly meetings where the CIPHER concepts continued to be explored and the framework was further developed. Additionally, task force leads were selected from the educator partners to coordinate the teams, including gathering data for future meetings.

Another outcome of iteration 2 was the decision to focus on K–12 partners for five months (September–January) before including additional business and industry collaborators in the design process. The following elements were identified in iteration 2 through focus group (task force) meetings as essential components to the next CIPHER iteration, both in the planning phase and in the initiative's design:

- *Building understanding among internal and external stakeholders*: At times, there was a marked dissonance about the meaning of cyber, cybersecurity, and computer science. The task force members overwhelmingly expressed the need for K–12 schools to have a common understanding of cybersecurity, career trajectories for students interested in cyberfields, and the preparation teachers need to lead courses in this area. CIPHER was seen as a mechanism to develop this common understanding across districts.
- *Unpacking cybersecurity and computer science*: In relation to developing a common understanding of cybersecurity among stakeholders, task force members described the need to better understand how school districts envision and teach cybersecurity and computer science.
- *Communicating and marketing*: Task force members discussed the necessity for focused, clear, and ongoing communication and marketing campaigns for CIPHER, including during the planning phase, to build interest in and support for the consortium.
- *Fostering hands-on professional development*: As noted, our educator stakeholders emphasize taking action rather than just "discussing" the possibilities for CIPHER. This dovetails with our DBIR approach and, as such, multiple professional development opportunities have been explored and are in the planning phases to be implemented in 2021. They will be used as a vehicle to build interest in CIPHER, provide needed skills to educators, identify areas of additional improvement for teaches and administrators, and gather critical information to develop the K–16 cyberpipeline.
- *Leading cyber in schools*: One area that was underdeveloped in the initial CIPHER design related to exploring the role of K–12 educational leaders. While our original goal was to support school-level leaders in their work leading effective and high-quality cybersecurity training programs, we have also come to better understand how different school districts are developing and implementing

cybersecurity curricula in classrooms. As a result, the CIPHER group needs to broaden its understanding of cybersecurity education leaders. In turn, as we work to identify those responsible for developing and implementing cybersecurity programs, we can enhance our support of their work and design development programs tailored to them.

- *Creating an advisory pipeline:* A final area that the task forces have emphasized is to help to create an advisory pipeline that will help students outline their pathways to cybersecurity careers.

Our findings from the first iterations of CIPHER show there is a strong desire among K–12 educators to partner with one another and with institutions of higher education to develop a cohesive approach to preparing students in the area of cybersecurity. In the subsequent months of the CIPHER planning phase, we intend to use the themes to further develop the model, which we anticipate will include incorporating high-school and college students into committees; host professional development sessions focused on cybersecurity (norming around a common understanding, curriculum design and instruction, and the development of academic pathways for students interested in cybersecurity) for teachers, professional school counselors, and administrators; and codesign curricular K–16 cybersecurity pathways for students. Because of our DBIR approach, we are able to design and implement the model while studying the efficacy of the effort and making iterative changes based on ongoing research.

Our hope is that this work will lead to fundamental findings about what administrators, educators, counselors, and parents need to know and be able to do to support cybersecurity education. The anticipated outcomes include the establishment of a CIPHER RPP that engages all stakeholders, a deep understanding of the current knowledge and infrastructure gap, and the creation of an inclusive model for K–16 cybersecurity education, which can be replicated nationwide to bring cybersecurity education to all students. ■

Acknowledgments

Correspondence concerning this article should be addressed to Karen L. Sanzo, at ksanzo@odu.edu. This work was supported, in part, by the National Science Foundation, under grant CNS-2012941. The authors would like to acknowledge the collaboration of Brian K. Payne, Chunsheng Xin, and Danella Zhao in securing the grant.

References

1. T. Anderson and J. Shattuck, "Design-based research: A decade of progress in education research?" *Educ. Res.*, vol. 41, no. 1, pp. 16–25, 2012. doi: 10.3102/0013189X11428813.
2. "Hack the gap," CyberSeek, Burning Glass, Boston, MA. Jan. 4, 2021. [Online]. Available: https://www.cyberseek.org/index.html
3. K. Evans and F. Reeder, "A human capital crisis in cybersecurity: A report of the CSIS commission on cybersecurity for the 44th presidency," Center for Strategic & International Studies, Washington, D.C., White Paper, 2010.
4. C. Ford, D. McNally, and K. Ford, "Using design-based research in higher education innovation," *Online Learn.*, vol. 21, no. 3, pp. 50–67, 2017. doi: 10.24059/olj.v21i3.1232.
5. M. Matheny, "CloudPassage study Finds U.S. Universities failing in cybersecurity education," CloudPassage, San Francisco, 2016. [Online] Available: https://www.cloudpassage.com/company/press-releases/cloudpassagestudy-finds-us-universities-failing-cybersecurity-education/
6. W. Zamora. "What K–12 schools need to shore up cybersecurity." Malwarebytes Labs Blog. https://blog.malwarebytes.com/101/2019/02/k-12-schools-need-shore-cybersecurity/ (accessed Dec. 1, 2019).

Karen L. Sanzo is a professor and graduate program director for the PK–12 Educational Leadership Program, Old Dominion University, Norfolk, Virginia, 23529, USA. Her research interests include school leadership development, creating and sustaining partnerships between universities and school districts, and the development and use of formative assessment practices in schools by leaders and teachers. She has served as principal investigator for several national and state-level grants in the areas of school leadership, formative assessment, and science, technology, engineering, and mathematics education. Contact her at ksanzo@odu.edu.

Jay Paredes Scribner is a professor of educational leadership at Old Dominion University, Norfolk, Virginia, 23529, USA. His research interests include professional and organizational learning and leadership. He has received awards for his research and contributions to the field of educational leadership from the National Staff Development Council, the University Council for Educational Administration, and the University of Wisconsin–Madison School of Education. In 2000, he was awarded a National Academy of Education postdoctoral fellowship. Contact him at jscribne@odu.edu.

Hongyi Wu is the Batten Chair of Cybersecurity and the director of the School of Cybersecurity, Old Dominion University, Norfolk, Virginia, 23529, USA, where he is also a professor in the Department of Electrical and Computer Engineering and holds a joint appointment in Department of Computer Science. His research interests include networked and intelligent cyberphysical systems for security, safety, and emergency management applications. He has served on the editorial board of several publications, including *IEEE Transactions on Mobile Computing, IEEE Transactions on Parallel and Distributed Systems,* and *IEEE Internet of Things Journal.* He received the National Science Foundation CAREER Award in 2004, the University of Louisiana at Lafayette Distinguished Professor Award in 2011, and the IEEE Mark Weiser Best Paper Award in 2018. He is a Fellow of IEEE. Contact him at h1wu@odu.edu.