Researchers say cybersecurity education varies widely in US

May 7 2024, by Tina Hilding

Credit: Pixabay/CC0 Public Domain

Cybersecurity programs vary dramatically across the country, a review has found. The authors argue that program leaders should work with professional societies to make sure graduates are well-trained to meet industry needs in a fast-changing field.

In the review, [published](#) as part of the *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1*, a Washington State University-led research team found a shortage of research in evaluating the instructional approaches being used to teach cybersecurity. The authors also contend that programs could benefit from increasing their use of educational and instructional tools and theories.

"There is a huge variation from school to school on how much cybersecurity content is required for students to take," said co-author Assefaw Gebremedhin, associate professor in the WSU School of Electrical Engineering and Computer Science and leader of the VICEROY Northwest Institute for Cybersecurity Education and Research (CySER).

"We found that programs could benefit from using ideas from other fields, such as [educational psychology](#), in which there would be a little more rigorous evaluation."

Cybersecurity is an increasingly important field of study because compromised data or [network infrastructure](#) can directly impact people's privacy, livelihoods and safety. The researchers also noted that adversaries change their tactics frequently, and cybersecurity professionals must be able to respond effectively.

As part of the study, the researchers analyzed programs at 100 institutions throughout the U.S. that are designated as a National Security Administration's National Center of Academic Excellence in Cybersecurity. To have the designation, the programs have to meet the NSA requirements for educational content and quality.

The researchers assessed factors such as the number and type of programs offered, the number of credits focused on cybersecurity

courses, listed learning outcomes and lists of professional jobs available for graduates.

They found that while the NSA designation provides requirements for the amount of cybersecurity content included in curricula, the center of excellence institutions vary widely in the types of programs they offer and how many cybersecurity-specific courses they provide. Half of the programs offered bachelor's degrees, while other programs offered certificates, associate degrees, minors or concentration tracks.

The most common type of program offered was a certificate, and most of the programs were housed within engineering, computer science, or technology schools or departments. The researchers found that industry professionals had different expectations of skill levels from what graduates of the program have.

The researchers hope the work will serve as a benchmark to compare programs across the U.S. and as a roadmap toward better meeting industry needs.

The oldest cybersecurity programs are only about 25 years old, said Gebremedhin, but programs have traditionally been training students to become information technology professionals or system administrators.

"In terms of maturity, in being a discipline as a separate degree program, cybersecurity is relatively new, even for computer science," said Gebremedhin.

The field is also constantly changing.

"In cyber operations, you want to be on offense," he said. "If you are to defend, then you need to stay ahead of your attacker, and if they keep changing, you have to be changing at a faster rate."

More information: James Crabb et al, A Critical Review of Cybersecurity Education in the United States, *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1* (2024). DOI: 10.1145/3626252.3630757

Provided by Washington State University