The New York Times | https://nyti.ms/2DoR1E7

How Do You Get Students to Think Like Criminals?

The skills needed for cybersecurity jobs aren't easy to learn in the classroom.

By Josephine Wolff
Ms. Wolff is an assistant professor at the Rochester Institute of Technology.

Nov. 14, 2018

Between September 2017 and August 2018, employers in the United States posted 313,735 job openings for cybersecurity professionals. Filling those jobs would mean increasing the country's current cybersecurity work force of 715,000 people by more than 40 percent, according to data presented at the National Initiative for Cybersecurity Education Conference this month. With the number of unfilled cybersecurity jobs worldwide projected to multiply into the millions in the next three years, it's no surprise that governments, companies and schools are racing to pour more resources into cybersecurity training and education programs.

As someone who teaches in a rapidly growing computing security program at the Rochester Institute of Technology, this is good news for me and my students. I think we are doing a good and responsible job of training our students, who will be snapped up by recruiters.

But I've watched as the field of cybersecurity has become formalized through a flurry of new degrees, certificates and curriculums, and I worry that some fundamental components of what make people really good at security — namely, the instincts to look at systems in unconventional ways and quickly identify possible ways to cause trouble — are being lost along the way.

The idea of degree programs focused solely on cybersecurity is still pretty new. At R.I.T., the bachelor's degree in security was introduced in 2007, and the dedicated Computing Security department wasn't formed until 2012. That means we haven't had a lot of time to debug these programs, especially since, in academic settings, every significant curricular change typically requires several meetings followed by extensive paperwork and committee approval.

The field is so new that nearly every cybersecurity professional over the age of 30 does not have a degree in cybersecurity — many of them don't even have degrees in computer science, and several don't have college degrees at all.

Cybersecurity has long been a field that embraced people with nontraditional backgrounds. Following the Equifax breach last year, some critics slammed the company for hiring a chief security officer who majored in music, prompting a considerable backlash from security professionals who took to Twitter to flash their own liberal arts degrees or lack of formal education.

The poster child for the unconventional path to a cybersecurity job is Kevin Mitnick, who was convicted of illegal computer hacking and spent five years in prison before establishing a career as a highly sought after security consultant.

It's not a coincidence that someone good at cybercrime would also be good at cybersecurity. After all, many cybersecurity jobs involve trying to think like a criminal to test the security of a software program, computer network or hardware device. Many of my students go on to work for red-teaming or penetration-testing firms, where they try to probe and attack computer systems from the outside to identify potential vulnerabilities.

Some of these skills can be taught in the classroom, through checklists of where to look for possible weaknesses and tools that can be used to help conduct those assessments. But the most effective red teams, like the most effective attackers, find vulnerabilities that no one has ever thought of before — much less included on a course syllabus.

The security technologist Bruce Schneier wrote an essay a decade ago about what he called "the security mind-set," or the ability to instinctively identify ways of subverting or compromising systems by using them in unexpected ways. "It's far easier to teach someone domain expertise — cryptography or software security or safecracking or document forgery — than it is to teach someone a security mind-set," he wrote.

Almost by definition, college classroom settings and the students who thrive in them are not a natural fit for the kinds of disruptive, rebellious and troublemaking instincts that lend themselves to finding new ways to compromise computers. It can be hard to reward those skills — much less teach them — in a college course where there are supposed to be clear expectations and learning objectives, well-defined grading rubrics and set schedules.

There are efforts to try to introduce these skills to the classroom, but they are few and far between. For example, the security researchers Gregory Conti and James Caroland published an article on what they called "Kobayashi Maru" assignments, named for a "Star Trek" training exercise, designed to force students to figure out creative ways to cheat. The example they used in their own class was an exam for which students were required to write down the first 100 digits of pi with very little notice. The students were expected (and encouraged) to cheat on the test but told that if they were caught, they would fail the exam. Of the 20 students in the class where this exercise was tested, all succeeded in cheating without being caught, much to their professors' delight.

There is plenty of useful and important material being taught in cybersecurity classes beside how to cheat, from programming and networks to cryptography, and my own area of economics and policy. But the students who graduate from our degree program in security often report that they got more out of their extracurricular security clubs and competitions than their coursework.

That may not necessarily be bad, or even unique to cybersecurity (don't get me started on the topic of how much I learned writing for my college newspaper), but it does suggest that as we race forward trying to train millions more people in cybersecurity to fill all the looming vacant jobs, there may be real gaps in the skills we know how to teach.

We should think carefully about the skills we need, about the rules and principles that we know how to teach and also about how to encourage students to break those rules and find ways around those principles.

Follow The New York Times Opinion section on Facebook, Twitter (@NYTopinion) and Instagram.

Josephine Wolff is an assistant professor of cybersecurity policy at the Tufts Fletcher School of Law and Diplomacy, the author of "You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches" and a contributing opinion writer. @josephinecwolff