The Post-Millennials Have Arrived!

New Approaches to Cybersecurity Education

Julie A. Rursch

The Pew Research Center last month signaled that the post-Millennial cohort (born 1997-present) is the latest generation [1] we will need to adapt course content for in higher education. As compared the Millennial generation which experienced the Internet boom, the post-Millennials are “always on” and “always connected.” Their world has always had access to social media and on-demand entertainment. Conversations can be held at any time, at any place, with anyone. These are the students we want to attract to fill cybersecurity careers.

One of the problems we have generally in education is, since many are likely part of the Boomer (born 1946-64) or Gen X (born 1965-80) generations, is that we teach linearly, processing one thing completely before moving on to the next while the Millennials (born 1981-96) and now the post-Millennials multi-task their thoughts and actions. As educators we have started to employ active learning activities in the classroom; think-pair-share (small group discussion), peer instruction exercises where one student is the “expert” and shares his/her knowledge with others. And, these activities work well in cybersecurity.

However, where we still are struggling is with providing students the ability to see how they can apply the skills being learned in the classroom, in the laboratory, and through homeworks in the after-college world. We know the post-Millennial generation is outcome-oriented. They need to be able to see the skills built through their classroom topics connect to future use of skills. Those of us who stand before them, construct the labs, and write the homework assignments tend to break the assignments and lectures into digestible pieces and forget to tie them all together with a final project or an overarching goal as we just work linearly through the week-by-week topics. We need to give students the bigger picture and help them see how the little part they are working on each week fits into their after-college goals.

As an example, let’s look at developing a realistic, hands-on experience with SQL injections, the number 1 item on the OWASP Top 10 List, to provide personal experience and connections to the real world. As faculty we can easily demonstrate the SQL injection concepts in class, both in code and as an active demonstration. We can ask them on an exam how to prevent SQL injections which should result in some answer like sanitizing, validating, and escaping the data. This works at Bloom's lowest level, knowledge. However, if we give them each a web server, tell them they are the administrator for that web site, and have them do both pentesting on their own server (so checking for all of the Top 10, network, and OS vulnerabilities), as well as a code review, they can more clearly see how the classroom experience ties to the after-college world. It also moves them into the application and sometimes analysis level of the taxonomy. I have had students tell me that they have had SQL injections demonstrated in a previous database class, but they never understood how to prevent it until they had the opportunity to try it on their own with their own web servers. And, if giving students the entire web site is too much all at once for the class level, we can start with code snippets that are contrived for the students' ease of learning and then use similar code in the overall web site to help them make the jump to the larger picture.

Similarly, giving students an entire network that is filled with vulnerabilities and letting them have the opportunity to evaluate, remediate, and then reevaluate gives them a realistic multiple machine environment in which to work. Again, there may have to be smaller pieces of the experience given to them at first and then give them the full network as a final project with similar problems. The point of both of these examples is to give them an experience that is as realistic as possible.

Further, every time a new topic is introduced in the classroom or lab a "current event" can be included. We seem to have no limit on real world cases to build our arguments. The perfect example this past semester was using Atlanta and their ransomware problems which not only allowed discussion of ransomware, but also discussion of good disaster recovery practices and the need for business continuity plans. The latter two are good business management practices that we don't always cover in cybersecurity courses. "Current events" can easily frame the week's topic in the classroom, lab, or homework.

Now, the realistic scenarios are difficult for faculty to generate and take a lot of time and energy. Likewise, faculty do not get rewarded for good teaching. They get rewarded for papers and conference attendance, even lecturers. So, there needs to be a shift in higher education to value the realism added to the classroom and to recognize the demands post-Millennial students are making for this kind of classroom experience.

The second issue that we need to address is the adversarial feeling in cybersecurity curriculum. To date, many of the extracurricular activities, and to a lesser extent the hands-on activities in the labs or homeworks, tend to focus on an attack mentality. As an underrepresented population, whether gender or ethnicity or other, it can be hard to put yourself into that role. We are already in the minority and then to work with cybersecurity there is a certain level of bravado that occurs with competitions and events like capture the flag or build and defend events. Even seemingly innocuous things like rank ordering teams or people in event can reduce someone's self-efficacy and, therefore, their interest in cybersecurity. Additionally, when I have been in meetings where these kinds of objections are raised I was basically told the students (in the case I am thinking about, girls) needed to, "Toughen up, buttercup!" That is not an acceptable answer. We come at cybersecurity from many backgrounds and many experiences. We won't attract a diverse population if we are chastised for offering a different view.

Finally, there isn't enough reflection in current cybersecurity education. Even if we are doing a good job and providing post-Millennial students with outcome-oriented projects where they can build future use skills, we don't have them spend enough time thinking about how what they just completed related to their major, relates to career choices, and relates to what they need to improve upon. Simple reflection questions added into the weekly assignments that ask students to put what they just completed into the larger world context is also valuable in helping them understand the tasks role in the real world.

[1] M. Dimock. (2018, March 2). *Defining generations: Where Millennials end and post-Millennials begin*. Available: http://www.pewresearch.org/fact-tank/2018/03/01/defining-generations-where-millennials-end-and-post-millennials-begin/