Breadth vs. Depth: Best Practices Teaching Cybersecurity in a Small Public University Sharing Models

Professor Frank H. Katz

ABSTRACT

In recent history, America witnessed cyber breaches at Snapchat, where employees had personal information stolen by way of a phishing scam; Premier Healthcare, which saw unencrypted data pertaining to more than 200,000 users stolen from a laptop; Verizon Enterprise Solutions, who had the information of 1.5 million customers stolen by hackers; and LinkedIn, who saw a 2012 data breach "come back to haunt them when 117 million e-mail and password combinations stolen by hackers four years ago popped up online [1]." These are just some of the many breaches experienced recently, which also included the hacking of a Presidential candidate by actors of a foreign nation-state, potentially an act of cyber warfare.

Who is going to protect US citizens from these threats? In January 2017, CSO Online reported that "A Forbes story in 2016 reported there would be 1 million cybersecurity job openings in 2017. Some things are worth repeating. There were 1 million cybersecurity job openings in 2017, give or take. Not much has changed over the past year. Can armies of interns close the cybersecurity skills gap asked a Fast Company story in September of 2016? Not likely. In the US, and internationally, there's not enough cybersecurity grads — or computer science grads with cyber credits [2]." This begs the question, "what constitutes the best practices in a cybersecurity program that will educate these future professionals?" What is the right balance between the breadth of the curriculum in such a program and its depth? This paper will attempt to answer those questions by describing how our university's NSA accredited program was created, the courses it contains, and the pedagogical methods it employs to educate and prepare future cybersecurity professionals for the workplace.

Frank Katz holds an M.S. in Management from Georgia State University (1987), and a B.A. in Computer Science from the University of Florida (1977). Upon graduating from Florida, he was commissioned a 2LT in the U.S Army, serving on active duty for four years, attaining the rank of Captain.

He has over twenty-one years of industry experience in the IT field working for companies as diverse as The Coca-Cola Company and Great Dane Trailers, Inc.

He has been an Assistant Professor at Armstrong State University, now Georgia Southern University, since 2002. While at Armstrong, he was instrumental in creating the curriculum in Cyber Security, which has been recognized as an NSA-CAE/CDE.

He has been published numerous times in Cyber Security, is an Editorial Board Member of Kennesaw State University's Journal of Cybersecurity Education, Research, and Practice, a member of ACM, and a Life Member of the Military Cyber Professionals Association.

Keywords—cybersecurity; cybersecurity education; pedagogy; curriculum; virtualization; stackable curriculum

I. HISTORY OF THE PROGRAM

When the Information Technology (IT) major was introduced at Armstrong State University (Armstrong) in 2002, there was no requirement that students take a course in either Computer or Information Security. Both Computer Science (CS) and IT students were required to take a course in Ethical Considerations in Computer Science, which has since been renamed as Introduction to Computer Ethics and Cyber Security. At the time, however, there was no course that addressed the growing field of Information Security. In recognition of this burgeoning field, in January 2006, Armstrong offered its first course in Information Security, approved as a permanent addition to Armstrong's IT curriculum. At the same time, Armstrong received funding for its Cyber Security Research Institute, a non-academic unit closely related to and funded by the U.S. Department of Homeland Security. The establishment of this research institute led the administration, the Department of Criminal Justice in the College of Arts and Sciences, and the (then) School of Computing to create an academic minor in cybersecurity to be cross-listed between Criminal Justice and Information Technology.

The curriculum would develop further, in October 2010, when the paper "Curriculum and Pedagogical Effects of the Creation of a Minor in Cyber Security" was presented at Kennesaw State University's Information Security Curriculum Development Conference (InfoSecCD), now named the Conference on CYBERSECURITY EDUCATION, RESEARCH & PRACTICE [3]. It described the issues related to the creation of an interdisciplinary minor in Cybersecurity at Armstrong, and its effect on

the university's IT major curriculum. At that time, we were not enrolling and graduating students in the minor because even though the second course in the minor had been created in the catalog, its curriculum had not been determined. Consequently, the conclusion of that paper left the fate of the minor in doubt, stating that much curriculum committee work needed to be done before the minor was either removed or properly and fully supported [3]. After attending the 2010 InfoSecCD, our department decided that the second course in cybersecurity would cover Network Security. As enrollment in the minor grew, including both IT and Criminal Justice students, we saw the need to expand our curriculum. Consequently, in the Fall of 2015, we offered our third course in cybersecurity, Ethical Hacking and Incident Response, making the minor even more robust.

II. STACKABLE CURRICULUM AS A MODEL FOR THE PROGRAM'S DEVELOPMENT

a. CACE and Potential Military Students

At this time, Armstrong created a Center for Applied Cyber Education (CACE). The Center is headed by a staff person with a military background in cybersecurity, CACE has several goals: (1) to coordinate engagement and cooperation in cybersecurity curricular efforts, such as having cybersecurity students mitigate a simulated attack, and having English/Journalism students report its findings in the student newspaper; (2) outreach to the community, as evidenced by CACE's running the Cyber Patriot program for local high school students in the Summer of 2016, and again in 2017; (3) marketing the university's cyber programs to potential civilian and military students; and (4) to engage in cyber workforce development.

Because Armstrong is located in Savannah, Georgia, near several major military installations, including the Army's Fort Stewart (3rd Infantry Division) and Hunter Army Airfield, enrolling military students was a priority. However, a challenge particular to that demographic was that military students might only be able to attend the university for just a few years before transferring to another installation. Since a student must be enrolled in a major degree program to earn a minor, this was seen as a major hurdle to overcome in enrolling military students in what was then Armstrong's sole cyber program, the minor in cybersecurity.

b. Stackable Curriculum as a Remedy

The concept of a stackable curriculum was identified as a means of resolving this challenge. Stackable curriculum, as defined in Portable, Stackable Credentials [4], allows students to earn shorter-term credentials with clear labor market value and then build on them to access more advanced jobs and higher wages. These stackable postsecondary certificates and credentials would offer an accelerated entrance to the job market; this is essential for students who need to work while in school and may not be able to wait four to six years to finally earn a marketable credential. "The majority (51%) of post-secondary

certificate programs take less than a year of instructional time to complete, while 41% take between one and two years Stackable credentials also increase the persistence and motivation of the learner by offering smaller, yet recognized subgoals [4]."

This academic concept is not new, but it was brand-new to Armstrong's Department of Computer Science and Information Technology, in which most of the courses in the minor were housed. To meet CACE's workforce development goals, we created the Undergraduate Certificate in Cyber Security, and an Associate of Science, Cyber Security Track for enrolled students not interested in earning a degree, and enrolled students majoring in various unrelated fields. We also modified the Bachelor of Information Technology (BIT) degree so to have a general IT Track and a Cyber Security Track. The premise in creating these programs was that if a student matriculated in the Certificate program, and then wanted to earn a degree, that student could earn the certificate, and then either earn the AS or BIT with the Cyber Security Track. Considered the first cybersecurity program for student enrollment, the certificate was created to only require six courses in IT and cybersecurity, with only one prerequisite – college algebra.

In the Spring semester of 2015, Armstrong began its year-long attempt to earn the coveted NSA-CAE in CDE designation. Armed with a curriculum that included four courses solely dedicated to Cyber Security and the Interdisciplinary Minor in Cyber Security program, this was a rigorous and time-consuming effort. Although the curriculum presented to the NSA-CAE reviewers was the Minor program that included cybersecurity, Armstrong included the nascent Undergraduate Certificate and AS in our application. Armstrong was awarded its designation in December 2015 and presented with the designation certificate at the National Cyber Summit in June 2016.

III. COURSES IN THE PROGRAM – BREADTH VS. DEPTH

In any educational setting, one of the great debates is whether a program of study provides both breadth and depth of knowledge in that curriculum. When teaching information security, one way of defining breadth is "where we want to ensure that our students understand fundamentals of the various components that are at play in information security [5]." This includes computing but also includes other disciplines, such as law, psychology, ethics, and communication skills. "Depth in this area is where we sacrifice some of that breadth for additional skills, training, and practice in some of the specific tools, skills, and knowledge directly related to the practice of a particular area of information security [5]."

a. Breadth of Education in Armstrong's Cybersecurity Programs

In "The Case for Depth in Cybersecurity Education", the authors state that "all CAE/IAE (Information Assurance Education, now CDE, or Cyber Defense Education) schools must map their curriculum to government information assurance standards. While these

standards provide a broad approach to teaching cybersecurity, employers increasingly desire depth and breadth of knowledge[6]." This implies that the NSA-CAE program's standards do not promote depth of knowledge in cybersecurity. Having gone through the process of becoming a CAE institution, this is not necessarily accurate. Armstrong's cybersecurity curriculum has breadth by taking a holistic approach in teaching cybersecurity, holistic in that learning cybersecurity is not just learning technology. Our curriculum integrates the "pillars of people, process, and technology[7]", as all three are crucial for implementing cybersecurity solutions. We accomplish this in many of our IT and cybersecurity courses through not just labs, but case studies, exercises, and role-playing scenarios involving non-technical aspects of the discipline. We teach various components of cybersecurity starting with the fundamentals of Computer Science, touching on it in courses on Operating Systems, Data Communications, Systems Analysis and Design, and Network Design and Administration. There is hardly a course in our IT curriculum, exclusive of our cybersecurity courses, which has not been mapped to the NSA-CAE Knowledge Units (KUs).

b. Depth of Education in Armstrong's Cybersecurity Programs

The depth of instruction in the curriculum is just as important. The article describes depth in cybersecurity education as starting in high school education, including competitive initiatives such as the Cyber Patriot program. These College competitions also lead to depth in education. However, depth can also be "supported and even inspired in a classroom; however, students must take what they learn and apply it independently. Classroom experiences that support depth must focus on the learner as opposed to the instructor; they must offer continuous assessment with rapid feedback and the ability for the learner to focus and direct their learning to meet current tasks[6]." Manson and Pike's research highlights "A 2009 Washington Post article covering the debate between depth vs. breadth in science education defined depth as focusing on a few topics so students have time to absorb and comprehend the subject vs. breadth as covering every topic so students can get a sense of the whole and can later pursue those parts they find interesting[6]."

Since the depth of cybersecurity education is so important, how do we support that principle in our curriculum? We do this in two ways: (1) by our courses, and (2) by the methods used to teach the courses. Our students begin their study of cybersecurity through two general courses: CSCI 2070, Introduction to Computer Ethics and Cyber Security, and ITEC 3700, Cybersecurity I, Fundamentals of Information Systems Security. However, the remaining courses in our curriculum support the principle of depth in education by focusing on just three topics: network security, ethical hacking, and cyber forensics. ITEC 4200, Network Security, focuses solely on endpoint security—the use of firewalls and VPNs to secure a network. ITEC 4300, Ethical Hacking, emphasizes the ability of a student to penetrate a network and conduct reconnaissance, hack it, and then learn how to defend

such a network. CRJU 5003U, Cyber Forensics, is taught by the Criminal Justice department. This course is part of our minor, and it emphasizes real-world labs which allow the students to use various laboratory tools to examine digital media looking for potentially incriminating evidence. In the Spring 2017 semester, we also introduced a special topics course in Cyber Warfare, taught by the Director of CACE. This course was such a success that it might be made a permanent course in our curriculum, although short of offering a major in cybersecurity, degree requirements in the current BIT cybersecurity track may force it to be offered in our undergraduate minor or certificate.

The second way we support the principle of depth is through our instructional methods. Benjamin Franklin said: "Tell me and I forget, teach me and I may remember, involve me and I learn [8]." In keeping with that principle, it is vitally important to include hands-on laboratory work in a valid cybersecurity curriculum. "Instructors may want to be imaginative and create their own case studies and laboratory exercises, but time, and especially in the current era, financial constraints, affect all faculty members [9]." Rather than build our own labs, we have chosen to use virtual online labs, originally provided by the publisher of our textbooks, Jones and Bartlett Learning, and more recently, by InfoSec Learning. Regardless of provider, the advantages of using virtual labs far outweigh the time, cost, and physical plant required to create our own labs. In addition, virtual labs, run in the cloud, enable our students to perform the labs and associated exercises from anywhere, especially at home. However, the best way that these labs encourage learning in depth is that they focus on the student rather than the professor. The student must navigate a prescribed set of exercises, and will either receive positive or negative feedback from the labs based on their success in performing the exercises. Both providers include lab quizzes and challenge exercises, which provide immediate feedback to the students. Also, not only do many of the labs progressively build on material learned from previous labs, but they are directly correlated, on a chapter by chapter basis, to the material taught in the classroom and the textbook.

c. Depth of Education—Repetitive Skill Development

Repetitive skill development is an important way of measuring the depth of a curriculum [6]. "In his book Outliers, Malcolm Gladwell describes the 10,000-Hour Rule as a key to success in any field through practicing a specific task that can be accomplished with 20 hours a week for ten years. Ongoing changes in technology and national security needs require aspiring excellent cybersecurity professionals to set a goal of 10,000 hours of relevant, hands-on skill development [6]." While it is not possible for our curriculum to provide 10,000 hours of hands-on work in cybersecurity, our labs do provide a measure of repetitive skill development. For each course, several of the labs use the same virtual machines and tool to perform different functions and analysis. In this way, the students become more familiar with the tools. For example, throughout the labs used in the Network

Security course, the students repeatedly use: a Windows Server attack machine; a Kali Linux attack machine; Nmap; Zenmap; Wireshark; netstat; ping; port forwarding and NAT; various different common protocols including FTP, SSH, HTTP, SMTP; and various different firewalls, including native Windows Firewall, the Linux-based Endian firewall, and the pfSense firewall; learning how to configure and use RADIUS for access control; and learning how to configure and use various VPNs, including the PPTP and OpenVPN tools. The repetitive use of these tools in different exercises provides an effective means of teaching cybersecurity to our students. In a survey of Network Security students taken at the end of the Spring 2017 semester, out of nineteen students: 78,9% agreed or strongly agreed that they "understood the learning outcomes of the InfoSec Learning labs; 89.5% agreed or strongly agreed that the "lab questions and required screenshots in the InfoSec Learning labs reinforced and supported the learning outcomes"; and 94.7% agreed or strongly agreed that they "learned the lab concepts from the InfoSec Learning labs."

d. Depth of Education – Scalability

Another benefit of using online virtual labs is their scalability. On January 5, 2017, it was announced that as of January 1, 2018, Armstrong would consolidate with Georgia Southern University, in Statesboro, Georgia. On that date, we changed from a university of approximately 7,000 students into one with about 29,000 students, the fourth largest university in Georgia. Georgia Southern does not have any undergraduate programs in cybersecurity, and will essentially be acquiring ours. As students currently enrolled at Georgia Southern discover the new cybersecurity programs, we expect their enrollment to increase. This may require an increase in online delivery of our cybersecurity courses. The need to scale up lab exercises to support our curriculum will be significantly enhanced by using virtual, online labs.

IV. CONCLUSION

Developing and implementing an effective cybersecurity education program must incorporate both breadth and depth of educational practices. An effective cybersecurity program in an organization or corporation does not exist in a silo. Similarly, breadth of knowledge is vital to a useful university cybersecurity program of study because a student must understand the totality of the field and how it interacts with many other disciplines. However, the depth of education in cybersecurity is just as important, if not more important, because it ensures that students receive instruction and skill development in specific topics needed to become entry-level practitioners in the field. Our program at Armstrong is well on its way to providing such a solid education, and will only grow as we consolidate with Georgia Southern University in 2018.

NOTES

1. Retrieved from J. Leary, (December 16, 2016), The Biggest Data Breaches in 2016, retrieved June 26, 2017, from https://www.identityforce.com/blog/2016-data-breaches.

2. Retrieved from S. Morgan, (January 8, 2017), One-million cybersecurity job openings in 2017, retrieved June 26, 2017, from http://www.csoonline.com/article/3155324/it-careers/1-million-cybersecurity-job-openings-in-2017.html?upd=1498495039447.

3. F.H. Katz, "Curriculum and Pedagogical Effects of the Creation of a Minor in Cyber Security," presented at the 2010 Information Security Curriculum Development Conference (InfoSecCD 2010), October 1-2, 2010, Kennesaw State University, Kennesaw, GA. Published in the proceedings of the conference and in the Digital Library of the ACM.

4. J.T. Austin, G.O. Mellow, M. Rosin, and M. Seltzer, "Portable, Stackable Credentials, A New Education Model for Industry-Specific Career Pathways," McGraw-Hill Research Foundation, 7, November 2012.

5. D. Burley, "Interview With Gene Spafford on Balancing Breadth and Depth in Cybersecurity Education," in ACM Inroads, March 2014, 42-43.

6. D. Manson and R. Pike, "The Case for Depth in Cybersecurity Education," in ACM Inroads, March 2014, 47-51.

7. J. LeClair, S. Abraham, and L. Shih, "An Interdisciplinary Approach to Educating an Effective Cybersecurity Workforce," presented at the 2013 Information Security Curriculum Development Conference (InfoSecCD 2013), October 12, 2013, Kennesaw State University, Kennesaw, GA. Published in the Digital Library of the ACM.

8. Retrieved on June 27, 2017 from http://www.goodreads.com/quotes/21262-tell-me-and-i-forget-teach-me-and-i-may.

9. F.H. Katz, "Measuring the Effectiveness of Instruction Based on Material From a Hands-On Workshop in Information Assurance," presented at the 2013 Information Security Curriculum Development Conference (InfoSecCD 2013), October 12, 2013, Kennesaw State University, Kennesaw, GA. Published in the proceedings of the conference and in the Digital Library of the ACM.