Enhancements to Cybersecurity Curricula to Support Behavioral Aspects of Cyber

Bruce D. Caulkins, Ph.D.

Institute for Simulation & Training (IST)
University of Central Florida (UCF)
Orlando, Florida USA
bcaulkin@ist.ucf.edu

ABSTRACT

A comprehensive cybersecurity education would cover the people, processes, and technology that protect our systems, servers, networks, and data. Over the years, much effort has been given to augment and teach the tools that provide cybersecurity for administrators and users. Firewalls, intrusion prevention systems, and anti-virus programs are just a few of the tools to which developers and subsequently, teachers, have given much attention in their work. A great deal of commercial and academic courses focus precisely on the tools themselves. Very few courses, however, focus on the human aspects of cybersecurity – user behavior, hacker motivations, cyber operator decision making, predictability of certain types of attacks, and so on. This paper explores the human side of cybersecurity education and the technologies and collaborative vectors that must be taken to be successful.

BACKGROUND

Cybersecurity issues have been around for decades (Warner, 2012). Over the years many cybersecurity-related training and educational programs have focused on teaching the required tools to address the general security challenges in cyberspace. Training in firewall installation and maintenance, data analytics, digital forensics, and server security are just a few of these needed courses. However, very little has been done in the teaching realm to address a critical component in cyberspace operations - the human element (Champion, Jariwala, Ward, & Cooke, 2014).

In 2015, the United States Department of Defense (DoD) recognized this issue as a major gap within its force structure. The U.S. DoD subsequently published a far-reaching cyber strategy document, which acts as a guide for the military's ongoing efforts to strengthen its cyber forces and organizations. This strategy also works to promote complementary initiatives like the National Initiative for Cyberspace Education (NICE) and the National Cyberspace Workforce Framework (NCWF) (DoD, 2015).

Additionally, President Trump signed an Executive Order (EO) on cybersecurity (EO 13800, dated 11 May 2017) that spells out United States' policy to strengthen the cybersecurity tools and education for the government, our critical infrastructure, and for the nation itself. In EO 13800 the Administration describes the issue of cybersecurity education, training and workforce development. They also underline the need to effectively "assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education" (USG, 2017). This holistic approach to education, while not new, underscores the requirement for educators at all levels to continue to advance cybersecurity concepts and tools in their schools.

In 2016, we looked closely at cybersecurity career preparation techniques that particularly focused on teaching the technological knowledge, skills, and abilities (KSAs) relevant to the ever present security challenges in cyberspace. We also discussed and noted the fact that recent studies suggested that cyber vulnerabilities and defenses had more to do with human elements than had historically been acknowledged and we therefore needed to address the human aspects of cybersecurity at all levels of schools worldwide (Waldrop, 2016). As our research began to take shape, we decided to conduct a series of surveys to scope the issues at hand.

We first performed a survey via Qualtrics, an online survey platform in early 2016. Participants were randomly presented three out of five possible case studies of real world incidents that occurred in the recent past. The case studies (shown below in Table 1) provided a variety of possible scenarios for the participants to consider when answering the questions about which technical and non-technical KSAs were relevant for the particular case study.

Of course, the case studies were only representative examples of well documented cyber attacks that had occurred recently. The ten technical and non-technical KSAs were chosen prior to the

survey and represented possibly relevant KSAs to the five case studies chosen. Most of our respondents were initially contacted via the United States Army's Functional Area 53 listserver, which boasts more than 1,800 active subscribers to its network of cyber and information technology specialists (USARMY, 2017).

Table 1. Cyber Case Studies (Leis, Badillo-Urquiola, Caulkins, & Bockelman, 2016)

CASE STUDY	CYBER AREA
DDOS	Distributed Denial of Service (DDoS) against banks, gov't agencies, and private websites
HACKING	Hacking attack by "cyber jihadists" against a French television channel
PHISHING	Bank robberies via spear phishing to install Carbanak malware
DATA LEAK	Personal data leak from Japan Pension Service
EMPLOYEE	Former employee accessed approximately 2,200 GM Finance customers' identification

117 cyber specialists responded to the survey, producing solid results. The table below describes the ten techno-centric and human-centric KSAs analyzed in our research work. Notably, "Criminal Psychology" and "Sociological Behaviors" were described by the participants as the most relevant human-centric KSAs. All five human-centric KSAs received some respondents finding them relevant in every scenario.

Table 2. KSAs analyzed (Leis et al., 2016)

Techno-centric	**Human-centric**
Antivirus Software	Human-computer interactions
Firewalls	Criminal psychology
Hardware	Biomechanics/ergonomics
Computer Programming	Sociological behaviors
Encryption technologies	Human performance

The results of the survey showed the need for increased education in the human centric aspects of cyber operations and cybersecurity. The results reiterated the requirement that training and educating cybersecurity specialists on the tools are critically important; however, the results also

underscored the fact that the human aspects of cybersecurity need to be considered in our schools at all levels.

APPROACH

Our approach focused on advancement for graduate level education through the use of advanced web delivered content to support both online and in-class lectures. We focused on the five classes within UCF's Modeling and Simulation of Behavioral Cybersecurity program. This 15 credit hour, graduate certificate program starts in the Fall term each year and concludes in the Fall term of the following year, following a cohort-style of education. Generally, most students conduct the entire program together in a cohort of sorts, which further enables the learning process. Each class builds on the previous classes, culminating in the Fall in a behavioral cybersecurity capstone class that features individual and group work. The program started in the Fall of 2015 and is currently in its third cohort year. The backgrounds of the students were varied, with approximately sixty percent of each cohort coming from a technical background (computer science, IT management, computer engineering, and so on) while the remainder came from disciplines like psychology and political science.

A few guest lecturers were used in the IDC 5602 ("Cybersecurity: A Multidisciplinary Approach") class in the Fall as well as in the Summer IDC 6600 ("Emerging Cyber Issues") class. The lecturers consisted mostly of guest lecturers from government, industry, and academia, who showcased the cybersecurity issues of the day.

Within this program's classes, each lecture was recorded using Instructure's Canvas content delivery tool hosted on cloud-based servers sponsored by the University of Central Florida (UCF). Canvas is a robust learning management solution (LMS) that allows teachers and students to discuss, chat, post, notify and work on individual and group projects over an online platform. We recorded lectures using the Canvas LMS as well, providing access to online students, working side-by-side virtually with their in-class counterparts. Students could view lectures synchronously or asynchronously or both. Synchronous (i.e., online as the class is in progress) collaboration was encouraged but not mandatory as many of the students worked full time in other jobs and were not available to view the online session synchronously or attend the classes in person. Those students

who chose to attend synchronously were able to easily contribute to the lectures through the use of a chat box within the Canvas conferencing tool.

We chose to combine the online and lecture ("mixed mode") sections within each course, allowing both types of students to benefit from the positive aspects of the separate and distinct modes of instruction. In group led discussions and writing assignments, we ensured that each group had at least one member from the online section of the class and one member from the lecture section of the class. Further, we endeavored to balance each group to have equal numbers of technical and non-technical specialists in them. Results in the courses and in the program overall were extremely encouraging, where the students generally felt that the program positively improved their job situations.

CONCLUSION

Our work focused primarily on the coursework that currently exists at the graduate level in the M&S of Behavioral Cybersecurity program at the University of Central Florida in Orlando. We will continue to modify the UCF courses' syllabi but will also look towards future collaborations with other academic institutions that have interest in this field. One exemplary example is Howard University. Howard University has a robust undergraduate plan for behavioral cybersecurity with whom we will continue to expand our work. While similar to UCF's program, the Howard University curriculum focuses more on encryption concepts and technologies and a few other issues. Collaboration with other universities within the Florida State University System (SUS) is ongoing as well. The Florida Center for Cybersecurity (FC2), located in Tampa, Florida, enables the statewide collaboration by working with "all State University System of Florida institutions, industry, the military, government, and the community to build Florida's cybersecurity workforce" (Cybersecurity, 2017).

Collaboration expansion with industry and government is needed as well. Our Modeling and Simulation of Behavioral Cybersecurity program needs to conduct underlying research to support various government programs that support our behavioral cybersecurity goals. The DoD's Persistent Cyber Training Environment (PCTE) is one such possible support program. We envision that PCTE related research and other research vectors would benefit our courses and in

turn, our students and instructors' research would greatly benefit these government programs by providing research to support the technical and behavioral aspects of their work.

REFERENCES

Champion, M., Jariwala, S., Ward, P., & Cooke, N. J. (2014). *Using Cognitive Task Analysis to Investigate the Contribution of Informal Education to Developing Cyber Security Expertise.* Paper presented at the Proceedings of the Human Factors and Ergonomics Society 58th Annual Meeting.

Cybersecurity, F. C. f. (2017). The FC2 Mission Page. Retrieved from http://www.thefc2.org/

DoD. (2015). *The Department of Defense Cyber Strategy*. Washington, D.C. Retrieved from http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Leis, R., Badillo-Urquiola, K., Caulkins, B. D., & Bockelman, P. (2016). *Modeling and Simulation Education for Behavioral Cybersecurity.* Paper presented at the Interservice/Industry, Training, Simulation and Education Conference (I/ITSEC), Orlando, FL.

USARMY. (2017). United States Army FA 53 Listserver. Retrieved from http://53list.army.mil/scripts/wa.cgi?INDEX

USG. (2017). *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Washington, D.C.: Executive Office of the President Retrieved from https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

Waldrop, M. M. (2016). How to hack the hackers: The human side of cybercrime. *Nature, 533*(7602), 164-167. doi:http://doi.org/10.1038/533164a

Warner, M. (2012). Cybersecurity: A Pre-history. *Intelligence and National Security, 27*(5), 781-799.