Open Access License Notice

The Collaboratory Experience: The Human Factor in Cybersecurity

Dahlia Handman, Ph.D.
dahlia.lynn@maine.edu

Raymond Albert, Ph.D.
ralbert@maine.edu

University of Southern Maine
P.O. 9300
Portland, Maine

Abstract - The Maine Cybersecurity Cluster (MCSC) at the University of Southern Maine in partnership with the University of Maine at Fort Kent, University of Maine at Augusta, and the York County Community College were awarded a two-year National Science Foundation grant during Fall 2014 to pilot an inter-institutional virtual cybersecurity collaborative learning laboratory, or "Collaboratory," establishing a shared educational environment. The Collaboratory, designed to highlight the interplay of technical and non-technical issues, hosted virtual simulations conducted over three semesters. The simulations challenged students to detect and respond to denial-of-service, data exfiltration, insider threat, and advanced persistent threat scenarios. As importantly, the virtual environment requires students to move beyond their technical expertise and understand the critical nature of human interaction and the importance of social tactics. This environment is providing Maine students across the state with the opportunity to gain practical, collaborative experience in preventing and mitigating cyber-attacks in real-time. This paper delineates the background and benefits of the Virtual Cybersecurity Collaborative Learning Laboratory (VCCLL), or Collaboratory.

Categories and Subject Descriptors

K.4.3 [Organizational Impacts]: *Computer-supported collaborative work*

K.6.5 [Security and Protection]: *Unauthorized access (e.g., hacking, phreaking)*

General Terms

Management, Security, Human Factors

Keywords

Cybersecurity, Information Security

1. INTRODUCTION

The Collaboratory model has the potential to significantly impact cybersecurity education and workforce development, by availing undergraduate students from very different educational backgrounds and geographic locations to engage in instructional activities that promote effective interpersonal, communication, collaborative, team-work skills, thereby increasing the pool of highly sought well-rounded cybersecurity graduates. While the literature speaks frequently to the need for inter-agency collaboration and cooperation there is little discussion of the interpersonal skills and collaborative abilities that are needed among students being taught or addressed. With the advances in the technological challenges and the need to overcome them, cybersecurity classes do not make the time to work with students on the communication, interpersonal and collaborative skills that are required (often called soft-skills, now in demand by most companies) to work in effective teams or collaborative groups. This raises questions about the need for broader (inter-agency) communication when cybersecurity courses must cover so much technical material that there is little or no time and perhaps limited emphasis for students to learn how to communicate effectively in order to successfully collaborate, especially in the context of complex and perhaps chaotic situations, where clear and trusted human communication is required.

2. HUMAN FACTORS

Central to cybersecurity education is the need for a collaborative approach that employs a combination of adult-learning-based philosophy, just-in-time topicality, hands-on immersion, practical application and ethical appreciation as well as

establishment of effective communication and collaboration skills in order to address cybersecurity threats to multiple systems, networks and scenarios.

Cybersecurity students are educated to address the ever-increasing number of cybersecurity threats and mitigate or extinguish the effects of attacks. The technical aspects of cybersecurity grow and become more sophisticated on a daily basis. Cybersecurity curricula that, more often than not, emphasizes technology knowledge and skills over soft-skills (now in demand by most companies) prepares graduates who are hobbled in their interpersonal skills development and abilities to effectively communicate, collaborate and contribute as team members. The literature speaks frequently to the need for inter-agency collaboration and cooperation [12], but there is little discussion of the interpersonal skills and collaborative traits that are needed among students being taught or addressed [2,5]. This creates questions around the need for broader (inter-agency) communication when cybersecurity courses must cover so much technical material that there is little or no time and perhaps limited emphasis for students to learn how to communicate effectively in order to successfully collaborate, especially in the context of complex and perhaps chaotic situations, where clear and trusted human communication is required. The problem is obvious. Without excellent human communication that builds collaboration, there will be little chance of effective communication among and between individuals and agencies (business and academia and government), particularly in the interconnected and interdependent world of technology, and cybersecurity. Bonabeau, stressed that although there is a need to continue to improve the technical aspects of cybersecurity, human behavior is almost always the weakest link in security [2]. Understanding that human element in the development of cybersecurity curriculum involves acknowledging the integration of tasks, teams and technology systems and the intersection of human roles, individual skills and abilities [3] in addressing critical information security problems.

Companies today are seeking employees who can protect their organization's systems, understand that threats exist and create a culture of security where the actions individuals take and their communication is designed to protect information become automatic and intuitive. Cybersecurity situational awareness is about the

people, process and technology aspects of all of the controls to better understand, manage and predict situations. It is through perception, comprehension, projection, and resolution that that teams may develop shared mental models and combine their experience and training to best address cybersecurity threats and attacks [10]. The logical extension of this is that students will need to work with each other using the technical terminology of IT and cybersecurity but will increasingly need to be able to communicate with experts from business, industry, government, and specialize agencies [12].

3. CYBERSECURITY CURRICULUM

Beach argues that "academic institutions should develop human factors, usability, and communication curricula to assist graduates in making security intuitive and reflexive for those outside the discipline." [4] Only two percent of the 121 National Security Agency-recognized Centers of Academic Excellence institutions included in the study required human factors courses for cybersecurity program completion [4]. Only a fraction of these courses emphasize the role of communication and collaboration in team approaches to maintaining cybersecurity.

We assert that technical expertise must be coupled with communication skills conducive to making individual behavior and team performance more transparent, enabling better coordination, better adaptiveness and effectiveness.

The emergence of interpersonal skills and collaborative abilities as a critical aspect of cybersecurity curriculum highlights the iterative and dynamic nature of teams and team members as individuals collaborate to complete tasks, developing and adapting through various interactions, developing mechanisms and processes that help define their collective roles and accomplish tasks [7].

Mittu, while making a point that questions remain about the interdependence within and among teams, organizations and systems, identified the need to better understand the limits of teamwork as cooperation, competition, boundaries, training and technology interact in interdependent environments [9]. This understanding should contribute to future innovations in cybersecurity education.

4. COLLABORATORY

The University of Southern Maine, The University of Maine at Fort Kent and the York County Community College have implemented an inter-institutional Virtual Cybersecurity collaborative learning laboratory. This is a shared educational environment availing students in different geographic locations the opportunity to gain practical collaborative experience in preventing, detecting, and responding to cyber-attacks in real-time through participation in virtual simulations. The Virtual Cybersecurity Collaborative Learning Laboratory (VCCLL) or Collaboratory comprises technical infrastructure, pedagogical models and essential inter-team and intra-team interactions by participants located over 350 miles apart in Maine. The participants are students from various social, economic and educational backgrounds, taught by three instructors in at least three different cybersecurity courses. The Collaboratory model is a virtual laboratory for achieving learning outcomes related to Protect and Defend cybersecurity scenarios.

A key innovation of the program is interactive and performance-based employment of a mastery model that scaffolds participants to successive levels of complexity, reflective thinking, communication mastery and problem solving. Central to the Collaboratory model is the opportunity for students to understand and appreciate the value of working in effective ad hoc teams in a highly decentralized laboratory learning how to communicate effectively on many levels and often at off hours or during extreme conditions. Students must become confident not only in their ability to communicate and collaborate but in the utilization of technologies that cannot yet convey the complete subtleties of human "in situ" interaction [8] as a critical factor in cybersecurity incident response members' success is their ability to function well within a team [11].

The Collaboratory hosts a simulated community referred to as BetaPort, a fictional coastal city in Maine. Three technology firms operate within BetaPort, each hosting their own websites and supporting a variety of common technology services (e.g., email services, helpdesk). Most of the firms have multiple websites: for placing orders, managing their supply chain, tracking trouble-tickets, etc. The number, type, and interoperability of services change as students are tasked to

address challenges posed by their respective firms within BetaPort. Students research what network services need to be offered by an entity both internally and to external users. The Collaboratory environment remains completely isolated from the Internet and institutional networks.

The physical structure of the Collaboratory consists of single centralized site that hosts the physical infrastructure that, in turn, hosts the virtual networks, computers and devices that comprise the technology foundation of each of the three firms. Two separate remote physical locations each connect to the central site through secure virtual private network (VPN) connections. Each remote location consists of five computers, each hosting remote-desktop connections over the VPN to the centralized site.

Each firm within BetaPort "employs" students to serve in different roles (e.g., system administrator, helpdesk administrator, network administrator). Roles are assigned to ensure that students affiliated with the same BetaPort firm are distributed across the three physical sites. This ensures their ability to effectively communicate and collaborate through technological means will be thoroughly challenged. Other, non-student staff play supporting roles (e.g., public relations officer) to provide a more realistic environment. All participants are provided a cell-phone for back-up communications in the event computer-based communications is disrupted.

A week before each simulation event, students spend half a day in pre-simulation "training" during which they model the techniques they will be expected to master during the actual simulation event. Each student is encouraged to establish communication with their respective firm colleagues and begin developing a sense of "normal" day-to-day operations while performing common tasks (e.g., creation of new user account, monitoring of network traffic). A company directory and operations manual containing common internal technical specifications and procedural guidance are provided to each student along with their own cell phone. Each participant engages in a debriefing experience upon completion of the simulation. They are asked to reflect upon and share their thoughts about the experience. Probing questions focused on the aspects of communication, collaboration, technology and each node's overall infrastructure performance and

general operation are asked. These observations are recorded and later analyzed to determine further improvements that can be made to the simulation environment and activities. Xiao, et. al., support the notion that communication briefings held before/after team activities can reduce communication breakdowns by creating a shared mental model (shared expectation about what information should be given and received), improving team members' understanding of upcoming tasks and enhancing coordination and cohesion [14].

5. BENEFITS

One of the key aspects of the Collaboratory experience is understanding the human network and the challenges of interpersonal communication. The robustness of the physical space and the technical infrastructure enables students to communicate by 1) conversing face-to-face with local peers (within and across teams) in standard conversational modes, one-to-one or in the small groups; 2) "chatting" live via online application; 3) using email; 4) using dedicated cell phones.

The model addresses both the technological aspects of the cyber training and "trust", which is often at the heart of all cybersecurity undertakings. This "trust" includes trusted systems, nodes, and identification, which are all subject to attack or subversion. As importantly, it also includes the trusting relationship among the students (student to student individually or in teams) or students to machine(s). The value of trust among team members is the contribution to increased information sharing, cooperation and decreased levels of conflict [13]. Without the interpersonal (and person to machine) trust developed by solid communication practices, collaboration will not take place or will dwindle rapidly.

Additionally, there are behavioral, affective and cognitive team processes that emerge as a result of the shared experience within the VCCLL. The pre-simulation before each event enables students to begin to develop a greater level of situational awareness of the task ahead and what collective efforts might be required to monitor the task environment. Developing shared awareness helps facilitate "sense making" and goal accomplishment in anticipation of the actual simulation ahead.

Macro cognition, or the process through which individual learning and information gathering activities are transformed into collective knowledge occur through the act of information sharing, exchange and the distribution of knowledge as the virtual scenarios unfold throughout the simulation [6]. Communication and coordination activities within the scenario experience provide students with a sense of collective accomplishment. Adaptive behavior is observed as students modify their thinking and conduct in response to the new and changing environment in the virtual Collaboratory.

As the interconnectedness of our society in cyberspace has grown exponentially, virtually every aspect of government, business and industry has become dependent on cyber networks and therefore on network security. This interconnectedness has increased the need for shared risk, and today communities of organizations must work more collaboratively and trust the intelligence they share.

The Collaboratory model exemplifies and avails significant gains in preparing the future cybersecurity workforce as a result of harnessing the synergistic potential among higher education institutions that collaborative and cooperate [1].

Kozlowski, et. al., discuss human system integration and its positive influence on enhancing coordination and teamwork [7]. Varieties of team processes comprise overall team cognition, including situational awareness and shared mental models. It is important for practitioners to consider the degree to which the information inputs a team will be utilizing during task performance are specialized, distributed, and how members are likely to combine their information together to produce outcomes [7]. Given the nebulous and specialized technologies faced by cybersecurity teams it is likely that members of the team will regularly interact through virtual means. Ensuring that such groups are capable of developing and maintaining efficient, effective processes for collaboratively planning for, acting upon, and evaluating events that occur in their task environment will be critical [7].

6. SUMMARY

Physical separation is a key concept in this project, both the geographical separation, which is highly correlated with the socio-economic and technical backgrounds of these students, as well as the "virtual distance" phenomenon, which means that students will be skilled and comfortable working with technologically intensive control operations that are symbolically available in some cases and physically available in others. Best practice in cyber security education has relied on the use of physical equipment, and at best the use of local, virtual networks and machines. The virtual cybersecurity collaborative learning laboratory model, the "Collaboratory", expands and enhances procedures and practices, filling gaps between the technical and non-technical issues in cybersecurity, via virtual and remote telecommunications in reliable and synergistic ways. Central to the Collaboratory model is that students understand and appreciate the value of working in virtual teams in a highly decentralized (geographically) virtual laboratory where they may or may not have peers on par with their own level of technical proficiency and expertise. Students must necessarily become confident in their ability to communicate and establish mutual trust in order to effectively and collectively make appropriate individual and group decisions to protect, defend, detect and recover from threats to information security. The model addresses both the technical aspects of cybersecurity education and social/behavioral aspects (e.g., "trust"), which is at the heart of most cybersecurity operations and undertakings.

ACKNOWLEDGEMENTS

This research is supported by the National Science Foundation as part of NSF Award -1438826 and we acknowledge the University of Maine System for its support of this project.

REFERENCES

[1] Albert, R.T., Bennett, C., Briggs, D., Ebben, M., Felch, H., Kokoska, D., Lovewell, L., MacDonald, C., Markowsky, G., Markowsky, L., Murphy, J., Sihler, E., Wilson, G., 2015. Experiences with Establishment of a Multi-University Center of Academic Excellence in Information Assurance-Cyber Defense, *Proceedings of the 2015 World Congress in Computer Science, Computer Engineering & Applied Computing Conference*. Available at http://worldcomp-proceedings.com/proc/proc2015/sam.html

[2] Bonabeau, E. March 24, 2011. Cyber-Security Can't Ignore Human Behavior. *The Atlantic*. Available at http://www.theatlantic.com/technology/archive/2011/03/cyber-security-cant-ignore-human-behavior/72826/

[3] Durso, F.T., Boehm-Davis, D.A., and Lee, D., 2015. *Handbook of Human Systems Integration. American Psychological Association*. Washington, D.C.

[4] Beach, S.K., 2014. Usable Cybersecurity: Human Factors in Cybersecurity Education Curricula. *National Cybersecurity Institute Journal*. 1,1 (2014), 5-21.

[5] Fallows, E. November 30, 2010 Cyber-Security, China, and SENDS. *The Atlantic*. Available at http://www.theatlantic.com/technology/archive/2010/11/cyber-security-china-sends/67191/

[6] Kozlowski, S.W.J., and Chao, G.T. 2012. *The Dynamics of Emergence: Cognition and Cohesion in Work Teams. Managerial and Decision Economics*. (June 1, 2012). 33: 335-354. Wileyonlinelbrary.com DOI: 10.1002/mde.2552.

[7] Kozlowski, S.W.J., Grand, J.A., Baard, S.K. and Pearce, M., 2015. Teams, Teamwork, and Team Effectiveness: Implications for Human Systems Integration. *APA handbook of human systems integration*. Washington, DC, US: American Psychological Association.

[8] Murphy, J., Sihler, E., Ebben, M., Lovewell, L., and Wilson, G. *Building a Virtual Cybersecurity Collaborative Learning Laboratory (VCCLL)*. The 2014 International Conference on Security and Management, Las Vegas, NV, July 21-24, 2014 (SAM14) 425-429, ISBN: 1-60132-285-2.

[9] Mittu, R., and Lawless, W.F., (2014). Human Factors in Cybersecurity and the Role for AI. Association for the Advancement of Artificial Intelligence. Foundations of Autonomy and Its (Cyber) Threats: From Individuals to Interdependence: Papers from the 2015 AAAI Spring Symposium.

[10] Onwubiko, C. 2015. Cyber Security Operations Centre: Security Monitoring for protecting Business and supporting Cyber Defense Strategy, *Proceedings of the IEEE*

International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA 2015), joint and co-located with Cyber Science 2015 conferences, London, UK.

[11] Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomasseti, A., Repchick, K., Zaccaro, S., Dalal, R. and Tetrick, L. 2015. Improving Cybersecurity Incident Response Team Effectiveness Using Team-Based Research. *IEEE Security & Privacy*. 13,4 (July/August 2015), 20-29.

[12] Viveros, M., and Jarvis, D. 2013. *Cybersecurity education for the next generation. Advancing a collaborative approach*. The IBM Center for Applied Insights. April, 2013. http:/www.ibm.com/developerworks/library/se-education/index.html

[13] Wildman, J. L., Shuffler, M., Lazzara, E. H., Fiore, S., Burke, C. S., Salas, E. and Garven, S. 2012. Trust development in swift starting action teams: A multilevel framework. *Group & Organization Management*, 37, 138-170.

[14] Xiao, Y., Parker, H.S., Manser, T. 2013. Teamwork and Collaboration. *Review of Human Factors and Ergonomics*, 8,1, 2013, 55-102