Journal of Cybersecurity Education, Research and Practice

Volume 2019 | Number 1 Article 6

June 2019

A Design Case: Assessing the Functional Needs for a Multi-faceted Cybersecurity Learning Space

Charles J. Lesko Jr.
East Carolina University, leskoc@ecu.edu

A Design Case: Assessing the Functional Needs for a Multi-faceted Cybersecurity Learning Space

Abstract

Following a multi-year effort that developed not only a detailed list of functional requirements but also the preliminary physical and logical design layouts, the concept for a multi-faceted cybersecurity center was approved and the physical, as well as, additional infrastructure space was subsequently allocated. This effort briefly describes the structure and scope of the current cybersecurity program being supported and then draws out the functional requirements that were identified for the center based on the needs of the institution's cybersecurity program. It also highlights the physical and logical design specifications of the center, as well as, the many external program delivery requirements that were identified as essential to not only the current cybersecurity program but also the projected future needs of the program and its supporting activities.

Keywords

cybersecurity, interactive learning environment, collaborative learning

Cover Page Footnote

No Footnotes or acknowledgements required.

INTRODUCTION

As our society conducts more and more of our lives online, the security of our digital information becomes even more critical. Online social networks, cloud-based applications, and mobile devices are creating a cyberspace that is reaching nearly every aspect of our daily lives. The networks and digital infrastructure supporting this cyberspace provides access to our homes, schools, hospitals, businesses, and industry. The ever-increasing need to build and refine safeguards to protect the safety and security of our key infrastructure is growing in importance each day and the need to educate and train cybersecurity professionals is proportional to the task.

Following a multi-year effort that developed not only a detailed list of functional requirements but also the preliminary physical and logical design layouts, the concept for a multi-faceted cybersecurity center supporting multiple learning modalities was approved and the physical, as well as, additional infrastructure space was subsequently allocated. To articulate this effort in more detail, there is a brief description of the scope of the current cybersecurity program being supported. Next, the functional requirements for a supporting cybersecurity center based on the needs of the institution’s current cybersecurity program are identified. Additionally, there is highlighted discussion regarding the many external delivery requirements that were identified during the needs analysis phase that were deemed essential to the current cybersecurity program and the projected future needs of the program and its supporting activities. Finally, there is a discussion of factors being considered as follow-on developments and capabilities for future consideration.

SUPPORTED CYBERSECURITY PROGRAM

The demand for brick and mortar space at any institution is high, so maximizing the use of this learning space for the cybersecurity program was considered crucial to this project as well. From a functionality perspective, the cybersecurity center was designed from the ground up to be accessible not only to cybersecurity academic programs but also to support other cybersecurity-related activities, workshops and competitions throughout the institution, as well as, various other partnering institutions and programs. The institution’s cybersecurity program is based on a four-year information and computer technology curriculum with concentrated focus areas in computer networking, systems administration, and cybersecurity. The cybersecurity coursework builds on a base of information technology fundamentals that includes advanced work in infrastructure, systems security and intrusion detection. Due to the technical nature of the course content, most of the cybersecurity courses include corresponding labs to further augment the student's learning and provide as many hands-on opportunities as possible. The program requires students to have an internship, and to complete a two-semester professional, teamed capstone project. The program also supports multiple industry alliances, related professional certifications as well as various cybersecurity competitions and workshops on a regular recurring basis. The institution's cybersecurity program is also designated as one of the National Centers of Academic Excellence (CAE) in Cyber Defense. The National Security Agency (NSA) works jointly with the Department of Homeland Security (DHS) to sponsor numerous two-year and four-year institutions in the CAE program with the goal of ultimately reducing vulnerability in our national information infrastructure through the promotion of higher education and research in cyber defense (National Security Agency, 2019).

CYBERSECURITY LEARNING SPACE FUNCTIONAL REQUIREMENTS

Following a two-year study and series of facilitated working sessions with key members of the cybersecurity program faculty and other key institutional stakeholders, a functional requirements listing was developed to support the development of a collaborative learning space or cybersecurity center designed to directly support the institution's growing cybersecurity program. Although the final design of this learning space could have taken many forms, there were some key characteristics that were considered essential for is effort. The designated learning space needed to:

- Accommodate Multiple Types of Learning. The cybersecurity center needed to accommodate as many types of learning as practical in supporting not only on-campus but also, online, blended delivery modalities.
- Reduce Computing Footprint. The cybersecurity center needed to reduce the computing footprint within the designated lab space and support a robust virtualized infrastructure. In this case, computing footprint refers to the amount of physical space that the computing hardware takes up within the learning space. Where practical, placing processing, memory and storage resources in locations away from the learning space generally is more secure and reduces noise, heat, and other distractions.
- Maximize Advancements in Wireless and IoT Access. The cybersecurity center needed to maximize advancements in wireless and access to Internet of Things (IoT) devices and applications.
- Support Cybersecurity Non-Curricular Activities. The cybersecurity center needed to provide support for cybersecurity non-curricular

> activities including individual and one-on-one learning opportunities; project teaming, and small project group meetings and presentations; program mentoring sessions; and cybersecurity workforce development workshops and competitions.

Accommodating Multiple Types of Learning

When designing this learning space, consideration of the differences between individual and group learning was essential. Many of the learning types considered for this learning space included: visual, verbal, logical, auditory, social; intrapersonal, and physical. There are key differences in perspective from a student seated at a specific workstation within the center and the seating of specific groupings of students in the center for each given class setting. Designing the cybersecurity center with the ability to table or group students further enables course facilitators and helps to promote teamwork and independent learning in subject themes. This flexibility also allows faculty to create focus areas within the center for competitive activities or provide more individualized instruction to smaller groups of students (Hilberg, Chang, & Epaloose, 2003). As a learning space, the cybersecurity center was thus required to not only accommodate standard lecture-based deliveries but also support small and large group learning opportunities allow cybersecurity faculty to engage in a variety of teaching and learning styles (Kobza, 2018); (Lucarelli, 2015).

To further refine this list of accommodations a detailed review of course deliveries was conducted. Maximizing the use of any academic space is an essential institutional requirement so course facilitators within the cybersecurity program umbrella were brought together for a series of work sessions to evaluate and identify courses that could benefit from a multi-faceted collaborated learning space for their respective course deliveries. From these sessions, 8-10 cybersecurity program courses were identified for each of the fall and spring academic terms. From these sessions, several aspects of the cybersecurity degree programs came to light regarding the functional needs for this new learning space. With the steady growth of online degree programs that in many cases mirror the existing cybersecurity degree programs, concepts such as virtualization built into the learning space infrastructure were considered essential to minimizing the impact of managing face-to-face course and lab delivery with those delivered totally online (Eliot, Kendall, & Brockway, 2018); (Calhoun, 2017); (Creutzburg, 2018). It was also noted that there are also added advantages for the purposes of both certification and accreditation where delivering the same fundamental content in both on-campus and online modes is essential to avoid the many challenges associated with online deliveries (Danbury, 2018) (McKenzie, 2017). From a course delivery perspective, several related aspects of cybersecurity curricular activity were also identified:

- Individual learning. Most of the cybersecurity curriculum required a collaborative learning environment in which cooperative computer-centric learning can take place, three key aspects were considered. The cybersecurity center needed to provide an environment where students not only felt challenged but also felt safe (in the sense that they could be open to express or question). The cybersecurity center needed to be in small enough student groupings that each student felt they could contribute. Based on space size, capacity and course delivery need, it was determined that the cybersecurity center would seat a maximum of (24) students at a given session (Hilberg, Chang, & Epaloose, 2003); (Kobza, 2018).
- Teaming, Research, and Groups. Several of the cybersecurity program courses including a year-long capstone project series required collaborative learning in teams and small groups. It was noted that teaming and small group learning sessions provides a environment where students can actively participate, and provides an opportunity for engagement by each member of the team. Small group learning allows students to develop problem-solving, interpersonal, presentational and communication skills, all beneficial to life outside the classroom (Race, 2001). Additionally, learning in teams and small groups further enables group diversity and students are better able to draw upon their past experiences and knowledge (Lee, Morrone, & Siering, 2018); (Chou & Frank, 2018). The grouping of students with specific workstations also assists faculty in monitoring student activity and assists in developing a logical understanding of the cyber-activity being monitored. It was further noted that grouping students helps establish parent-child dependencies between network and various online lab elements of various simulated and online infrastructure and other IoT; thus, minimizing, redundant alerts and aiding students and faculty in understanding the impacts of faulty elements (Zeng, Deng, Hsiao, Huang, & Chung, 2018).
- Online “Hands-on” Lab Experiences. Since most of the cybersecurity curriculum required both physical and virtual cybersecurity lab experiences, online or virtual “hands-on” lab experiences were deemed essential for the learning space and the supporting infrastructure needed to be securely accessible from not only with the cybersecurity center, but also from off campus as well campus (Said, 2018). Current faculty noted that existing cybersecurity program laboratory solutions typically require significant effort to build, configure, and maintain and often do

not support reconfigurability, flexibility, and scalability; thus, the need to maintain a singular solution that can be utilized both on and off. Other cybersecurity program course capabilities include supporting the requirement for network and analytic diagnostics. Through logically connected current infrastructure resources, the cybersecurity center will provide students with the ability to present and analyze network health and performance statistics such as: interfaces facing maximum utilization; node response times, packet loss rates, CPU loads, memory usage, etc. Additional capability includes providing the ability to map and monitor network resources and their availability; as well as, to discover critical network devices, interfaces, servers, and other research data collection nodes. Finally, managing alerts regrading simulated and monitored research network activities. Alerts include availability statistics, performance metrics including device fault tolerance, errors and discards, hardware thresholds, syslog messages, and SNMP traps.

- Blended Learning and Video Conferencing. Within the context of the existing cybersecurity program, the concept of blended learning describes the way online program resources are being combined with traditional classroom methodologies and independent study opportunities to create a hybrid delivery approach. The proposed cybersecurity center learning space would need to support both synchronous and asynchronous classroom and laboratory activities (Calhoun C. , 2017); (Yekela, Thomson, & Niekerk, 2017). The ability to interact synchronously from the cybersecurity center with other off-site students or faculty necessitated the need for video conferencing capability. This necessitated the need for multiple overhead ceiling mounted video cameras with overhead microphone and speaker solution to maximize the audio and video coverage in the learning space. Additionally, the video conferencing capability provides the ability to: record onsite sessions; conduct synchronous blend-learning sessions; conduct online workshops and competitions; and supports the ability to conduct online mentoring sessions for both individuals or groups.

Reduce Computing Footprint

Collaborative learning spaces that incorporate virtual technologies allow for rapid emulation of multiple scenarios and infrastructures; an essential component to realizing an effective learning space for our cybersecurity program. Virtualized infrastructure is not only flexible in that student stations can be unique for each different course offering, but also it can reduce cost and setup and maintenance time for these key technical resources (Justice & Vyas, 2017); (Allison & Turner, 2017); (Kongcharoen, Hwang, & Ghinea, 2017). To meet the functional needs of the collaborative learning space, the technical requirements for the cybersecurity center demanded a supporting, on-premise, robust data center solution that abstracts the physical hardware from the pre-existing and augments existing institutional computing resources. Providing a virtualized solution for this space provides a powerful capability to dynamically allocate processing capacity, memory and storage to the various applications as needed. To not only maximized the utilization of these technical resources but also ease the administrative and resource lifecycle tasks that come with hardware deployments, a dedicated hyper-converged infrastructure (HCI) solution was selected to directly support the cybersecurity center (VMWare, 2018). From a physical layout perspective, it was determined that the HCI solution footprint would be located in a separate physical space from the cybersecurity center to ensure the appropriate security and climate control perimeters are maintained for the HCI solution and to reduce the noise footprint in the cybersecurity center itself.

By their very nature, cybersecurity labs and training activities can be volatile and menacing toward institutional infrastructure resources. To avoid conflicts with existing institutional infrastructure assets, the HCI solution was isolated both physical and logically from the existing institutional infrastructure resources. The HCI solution for the cybersecurity center was designed to provide the competition-style infrastructure environments needed when conducting cybersecurity workshops and competitions; these environments will be implemented by using various existing infrastructure solutions to emulate multiple gaming and research network infrastructures. Software services are supported by a significant deployment of VMware technologies that provides a scalable software-as-a-service environment to meet the specific needs of the cybersecurity center workstations. To provide this capability, students and facilitators are provided access to specially architected virtual machines (VMs). VMware vCloud Director cloud computing system, and Linux-class VMs are used to support most of the cybersecurity program courses be offered in the cybersecurity center (VMware, 2018).

Maximize Advancements in Wireless and IoT Access

The cybersecurity center will require access to enough virtualized IoT to facilitate the delivery of several cybersecurity-centric course labs. Wireless support for faculty and students to BYOD (Bring Your Own Device) must also be provided to include not only power and infrastructure connectivity (both wired and wireless), but also support labs involving various mobile interactive short-range protocols including Bluetooth, Zigbee, Z-Wave, WIFI and Thread (MacCallum, Day, Skelton, & Verhaart, 2017); (Song & Kong, August 2016). Several course facilitators also noted the need for their course deliveries to incorporate various development boards such as: Arduino, Raspberry Pi, and Intel Edison Board.

Support Cybersecurity Program Non-Curricular Activities

From a cybersecurity program perspective, several non-curricular activities were identified as critical to the program's success. When not in use as a course delivery space, the cybersecurity center will serve as a focal point for all interested in the cybersecurity program. When not in use as a course delivery space will remain open and available for use by both students, faculty and cybersecurity researchers. Proposed supported activities include:

- Program Mentoring. The cybersecurity center will maintain an onsite cybersecurity mentor to assist cybersecurity program students individually or in small study groups. The center will also provide the opportunity for students to informally meet and interact. The needs of numerous cybersecurity program course such as cybersecurity capstone, network operations management, involving teaming of students or session grouped discussions was considered crucial to the center's success and having a space available to team and interact with existing infrastructure is key.
- Cybersecurity Workforce Development, Competitions and Workshops. The current cybersecurity program supports several cyber-security-centric competitions and workshops. Designing the space to accommodate many of these events and provide a venue for delivery and demonstration was a key identified need (Dawson, Wang, & Williams, 2018); (Pusey, Gondree, & Peterson, 2016).
- Cybersecurity Knowledge Center. Finally, to help students to increase their knowledge level and skills, the cybersecurity center will focus on finding and digitally retaining knowledge resources and provide a focal point for student and faculty research.

PHYSICAL LAYOUT OF COLLABORATIVE LEARNING SPACE

As outlined in Figure 1, the cybersecurity learning space will contain (24) student workstations consisting of four integrated tables supporting six students each. To maximize the student's sense of space and to increase centralized visibility of student monitors to the faculty, each student station is slightly angled to the center aisle. The (4) six-station student tables also provide the room with the ability to sub-divide student efforts for teaming, operational game simulation, and group discussions. The virtualized HCI solution supports student access to course specific virtual machines, with course required Windows and Linux-based software tools that are pre-installed.

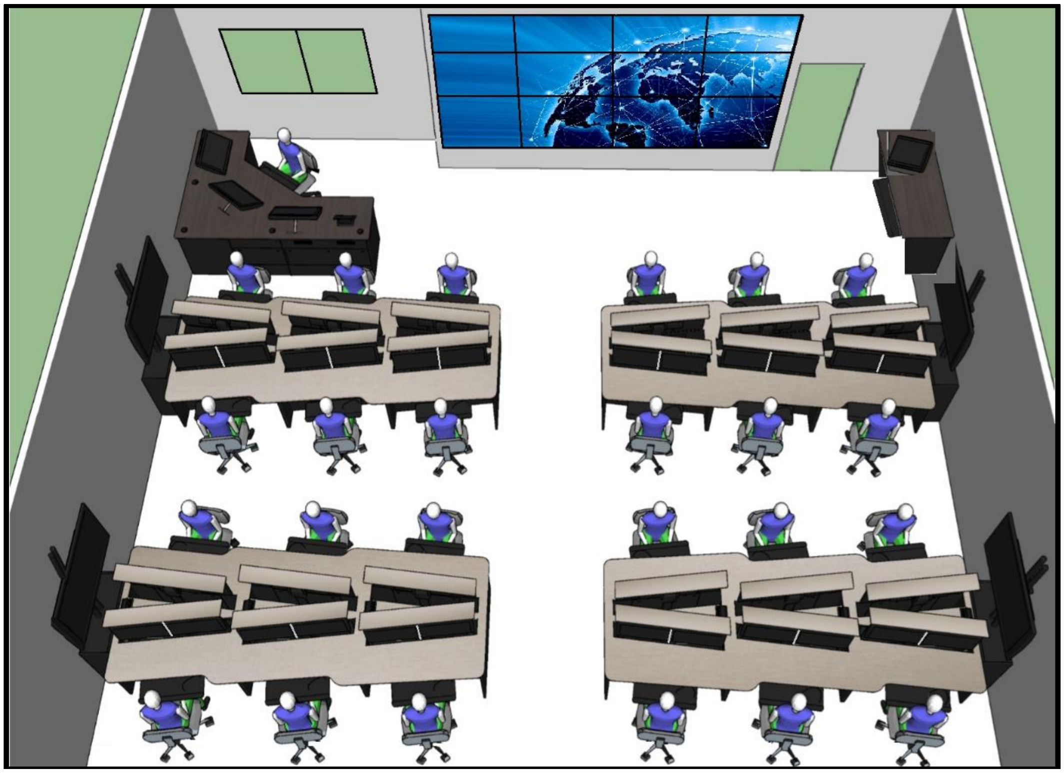

Figure 1: Physical Layout of Collaborative Learning Space

The cybersecurity center is directly supported with its own dedicated HCI solution enabling students to work in teams on single student specific VM's at the same time and the student's screens can be presented on either the table monitor located at the ends of each table or on the large wall screen display located at the front of the learning space. The HCI solution also supports the need to quickly transition from one course to another (hour by hour) throughout a given academic day. Course baseline virtual images can be created upfront to ease course and lab development efforts and once the desired view is attained it can be cloned as required. Each of the (24) student stations capabilities include:

- Dual-Monitor and Zero-Client Support. An all-in-one zero-client with dual monitors for each student's station with HCI providing multiple VM capability as predesigned per course or lab requirement. The HCI virtual solution allows students have access to not only multiple operating system VM's but also unique network infrastructures that are pre-configured for each course delivery. It should be noted here that many of these virtual configurations are cloned for use in mirror online courses as well. Each student's station has its own dedicated VM's and VM persistence is generally available for a continuous look and feel through the course or lab delivery.

- Table Presentation Monitors. Each of the four tables has its own large screen monitor as highlighted in Figure 1. The monitor is driven by its own thin-client and supporting VM. Students at the table have direct access to that VM to present whatever information deemed appropriate. Students can also present visuals from their own station or from a connect BYOD.
- Trolley Mounted Monitors. To remove the monitors as an obstacle to any grouped discussions, the dual monitors at each student's station can be lowered by either the student individually or at the mentor station which has class control of all student stations individually or collectively. This also facilitates courses where BYOD is the preferred environment. Note that Figure 1 shows the monitors in the up position.
- Individual Access Ports and Power Station. Each student's station has its own power station for powering up student owned laptops or other mobile devices. Additionally, at each station students have both hardwire (RJ45) connectivity to the center switches as well as dedicated Wi-Fi and Bluetooth connectivity for mobile devices utilized within the learning space. Each station is also provided with USB power outlets and USB access ports to their respective thin-clients for ease of access. The power station also provides access to thin-client peripherals such as voice and speaker.
- Mentor Station: As indicated in Figure 1, there is a single mentor station located at the front and to the left of the wall monitor. The mentor station is designed to either support the facilitator during course deliveries or support a lab mentor (usually a senior or graduate assistant) for non-course session times including after-hours mentoring, open lab time, and online course support. Controls for raising and lowering student station monitors are at the mentor station and advanced features supporting the wall screen can be managed from this station as well. Video conferencing is also managed from this station. Finally, the detailed wall screen controls can be set from this mentor station, but these controls are also available to the faculty wirelessly via a handheld device. It should be noted here that there is no lectern planned for this space. The physical layout allows for central flow and visibility from the center of the learning space, so faculty can best engage and collaborate with the class as either individuals or groups.
- Wall Screen. The cybersecurity learning space supports a full 16' by 7' (4 monitor by 3 monitor) wall screen monitor for large screen display located at the front of the learning space. The wall screen supports multiple

configurations for presentation. Several common wall screen views include: a full screen ‘lecture’ view with all twelve monitors presenting a singular image; that image coming from any number of sources including any active VM’s housed within the HCI solution. A second wall screen configuration could present lecture material in a 3 x 2 lecture view with the bottom four monitors replicating what is being presented at each team station. A third example competition view shows the space divided into two teams (Purple and Gold) with individual tables or specific student workstations being presented in the bottom four screens. Finally, the Lecture and WebEx example show a 3 x 3 screen for lectured content with video conferenced content in the right three monitors.

KEY CONSIDERATIONS ADDRESSED AND FURTHER LEARNING SPACE RESEARCH

In retrospect, there were several key areas of consideration when building out a multi-faceted-cybersecurity learning space. As noted, the demand for brick and mortar space at any institution is high, so to maximize the use of these cybersecurity program learning spaces it is crucial that the needs of the program are clearly understood and that scalability is built into the space, where practical. Although the final design of any given learning space can take on many forms, some key characteristics that were considered essential for is type effort include: accommodating multiple types of learning; reducing the computing footprint; maximizing advancements in wireless and IoT access; and supporting cybersecurity non-curricular activities. Additionally, the physical layout of these collaborative learning spaces should maximize the student’s sense of space while increasing centralized visibility of student activities to the faculty.

In designing in accessibility, the cybersecurity center design has been guided by various state and federal regulations as well as Section 508 of the Rehabilitation Act (29 USC 795d) and Web Content Accessibility Guidelines. All student stations meet established wheelchair standards for height and accessibility. It has been proposed that the student station closest to room entry be designated to support the additional needs of visually impaired students including screen reader software; braille keyboard and embosser at this station. Recent surveys by the National Federation of the Blind estimate that over 3.8 million people ages 16-64 have some level of visual disability. That equates to about 1.9% of the working age U.S. population (National Federation of the Blind, 2018). Providing accommodations for this population is an ongoing challenge and the cybersecurity center needs to build on that challenge. Working with the institution’s office for disability support and other supporting institutions and researchers, the center faculty have begun to identify technologies and space requirements that will assist the visually impaired at the cybersecurity center. Cybersecurity education is also a critical element to pass on to this population (Inan, Namin, Pogrund, & Jones, 2016).

Understanding the future logistics of the cybersecurity center will require a significant level of pre-planning, coordinated efforts in infrastructure development, and significant consideration towards time management for the center to maximize its capability. Centralizing the needs for a dedicated center planner as well as guidance for the selection and training of the center's designated mentors will also require further discussion and development of standard guidelines.

REFERENCES

Allison, M., & Turner, S. (2017, April 27). Designing a community aware virtual learning infrastructure for STEM. *2017 IEEE Integrated STEM Education Conference (ISEC)*, pp. 30-33.

Calhoun, C. (2017). Incorporating Blended Format Cybersecurity Education into a Community College Information Technology Program. *Community College Journal of Research and Practice, Volume 41, Issue 6*, 344-347.

Calhoun, C. D. (2017). Incorporating Blended Format Cybersecurity Education into a Community College Information Technology Program. *Community College Journal of Research and Practice, VOlume 41, Issue 6*, 344-347.

Chou, M., & Frank, J. (2018). Designing of Online Communities of Practice to Facilitate Collaborative Learning. *2018 5th International Symposium on Emerging Trends and Technologies in Libraries and Information Services (ETTLIS).* Noida, India: IEEE.

Creutzburg, R. (2018, January 28). Cybersecurity and Forensic Challenges - A Bibliographic Review. *Electronic Imaging*, pp. 1-16.

Danbury, S. (2018). *The big face-to-face versus online training debate.* Chicago, IL: Kineo.

Dawson, M., Wang, P., & Williams, K. (2018). The Role of CAE-CDE in Cybersecurity Education for Workforce Development. In S. Latifi, *Information Technology – New Generations, Advances in Intelligent Systems and Computing* (pp. 127-132). New York, NY: Springer International Publishing, AG.

Eliot, N., Kendall, D., & Brockway, M. (2018). A Flexible Laboratory Environment Supporting Honeypot Deployment for Teaching Real-World Cybersecurity Skills . *IEEE Access (6)*, 34884 - 34895 .

Hilberg, R., Chang, J.-M., & Epaloose, G. (2003). *Designing Effective Activity Centers for Diverse Learners: A Guide for Teachers at All Grade Levels and for All Subject Areas.* Santa Sruz, CA: Center for Research on Education, Diversity & Excellence.

Inan, F., Namin, A., Pogrund, R., & Jones, K. (2016). Internet Use and Cybersecurity Concerns of Individuals with Visual Impairments. *Educational Technology & Society, Volume 19, Issue 1*, 28-40.

Justice, C., & Vyas, R. (2017). Cybersecurity education: RunLabs rapidly create virtualized labs based on a simple configuration file. *ASEE Annual Conference and Exposition.* Columbus, OH: Proceedings for American Society for Engineering Education.

Kobza, C. (2018). *5 Tips for Active Learning Space Design.* Louisville, CO: Educause.

Kongcharoen, C., Hwang, W.-Y., & Ghinea, G. (2017). Synchronized Pair Configuration in Virtualization-Based Lab for Learning Computer Networks. *Journal of Educational Technology & Society , Volume 20, Number 3*, 54-68.

Lee, D., Morrone, A., & Siering, G. (2018). From swimming pool to collaborative learning studio: Pedagogy, space, and technology in a large active learning classroom. *Educational Technology Research and Development, Volume 66, Issue 1*, 95-127.

Lucarelli, A. (2015). *Optimizing the Physical Learning Environment for Cybersecurity Education and Training: A Collaborative Design Initiative.* Largo, MD: National CyberWatch Center.

MacCallum, K., Day, S., Skelton, D., & Verhaart, M. (2017). Mobile Affordances and Learning Theories in Supporting and Enhancing Learning. *International Journal of Mobile and Blended Learning (IJMBL), Volume 9, Issue 2*, 13.

McKenzie, L. (2017). *Questions on Quality of Online Learning.* Washington, DC: Inside Higher Ed.

National Federation of the Blind. (2018). *Statistical Facts about Blindness in the United States.* Baltimore, MD: National Federation of the Blind.

National Security Agency. (2019, January 2). *National Centers of Academic Excellence*. Retrieved from nsa.gov: https://www.nsa.gov/resources/students-educators/centers-academic-excellence/

Pusey, P., Gondree, M., & Peterson, Z. (2016). The Outcomes of Cybersecurity Competitions and Implications for Underrepresented Populations. *IEEE Security & Privacy, VOlume 14, Issue 6*, 90-95.

Race, P. (2001). *The Lecturer's Toolkit: A Practical Guide to Learning, Teaching & Assessment.* New York: Psychology Press.

Said, S. (2018). *Pedagogical Best Practices in Higher Education National Centers of Academic Excellence / Cyber Defense Centers of Academic Excellence in Cyber Defense.* Jackson, TN: Union University.

Song, Y., & Kong, S. C. (August 2016). Affordances and constraints of BYOD (Bring Your Own Device) for learning and teaching in higher education: Teachers' perspectives. *The Internet and Higher Education, Volume 32*.

VMWare. (2018, July). *Hyperconvergence* . Retrieved from Techtarget.com: https://searchconvergedinfrastructure.techtarget.com/definition/hyper-convergence

VMware. (2018, Aug 16). *VMware Horizon View*. Retrieved from Techtarget.com: https://searchvmware.techtarget.com/definition/VMware-Horizon-View

Yekela, O., Thomson, K.-L., & Niekerk, J. v. (2017). Assessing the Effectiveness of the Cisco Networking Academy Program in Developing Countrie. In M. Bishop, M. N. Futcher L., & M. Theocharidou, *Information Security Education for a Global Digital Society - IFIP Advances in Information and Communication Technology, Volume 503* (pp. 27-38). Rome, Italy: Springer, Cham.

Zeng, Z., Deng, Y., Hsiao, S., Huang, D., & Chung, C.-J. (2018). Conceptualizing Student Engagement in Virtual Hands-on Lab: Preliminary Findings from a Computer Network Security Course (Abstract Only). *Proceedings of the 49th ACM Technical Symposium on Computer Science Education* (pp. 1073-1073). Baltimore, MD: Association of Computing Machinery.