Transforming Cybersecurity Education through Consulting

Giti Javidi[1*] and Ehsan Sheybani[2]

[1] *Information Technology & Cybersecurity, University of South Florida*
[2] *Information Systems and Decision Science, University of South Florida*

[1]*javidi@usf.edu*, [2]*sheybani@usf.edu*

Abstract

Cyber Security is a total business problem. Creating meaningful learning experiences to prepare students for complex cyber situations in an organization is no small undertaking. The higher education is ill prepared in meeting the challenge of providing learning experiences that provide both breadth and depth. To fill the void and meet the fast-growing demands in cybersecurity workforce, the authors of the paper propose consulting experience as a strategy to create student-driven learning. Student-led consulting will assist students in systematically assessing organizational security problems and designing and implementing organizational interventions. We describe why college students should be equipped to conduct consulting projects with faculty supervision and how it can be done.

Keywords: *Cybersecurity education, soft skills, student-led consulting, e-shaped students, employability skills, experiential learning, consulting model*

1. Introduction

Cybersecurity is a fast-growing profession, and multi-skilled, talented graduates are in very high demand. The cyber security skills shortage is reaching prevalent proportions (Assante & Tobey, 2011; Lee; Bagchi-Sen; Rao & Upadhyaya, 2010; Javidi & Sheybani, 2019; Informationweek.com, 2019; Bishop & Irivine, 2010). The education system today is ill prepared to meet the challenge of producing an adequate number of cybersecurity professionals who are equipped with necessary skills for this complex profession. Malcom Gladwell (2013) argues that to be equipped with skills in any profession, 10,000 hours of practice is a necessary element. He describes the 10,000-Hour Rule, as simply a matter of practicing a specific task that can be accomplished with 20 hours of work a week for 10 years (Gladwell, 2013). 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 (Gladwell, 2013).

Educators, scholars and practitioners are now more than ever concerned about the gap between what students are being taught in school and the skills required for them to thrive in cybersecurity workforce. In our view, faculty can narrow this gap by creating opportunities for students to gain work experience needed by the field. "Without a rich background of experience, many aspects of cybersecurity are difficult to grasp" (Robinson, Lloyd Sherwood & DePaolo, 2009). In addition, many organizations claim that today's graduates lack the soft skills needed to succeed in their careers. This issue becomes more critical in cybersecurity field since there is not only a shortage of technical savvy professionals to fill cybersecurity roles but there is also a dearth of cybersecurity job applicants who

[*]Corresponding Author

possess the soft skills, such as strategic planning, change management, and human cognition and behavior. These limitations have the potential to invite fundamental issues in developing and implementing a successful cybersecurity strategy in a real-world situation since behind every malicious string of code or data-theft device is a person with his or her own strengths and weaknesses. Likewise, cybersecurity professionals must be aware of their own abilities and biases if they wish to stay a step ahead of any threat. Authors of this paper argue that some of these concepts can be taught in the classroom via labs and simulations but nothing can take place of real world experience where students can interact with actual clients to not only solve real world complex problems but to also gain deeper understanding of important concepts such as human cognition while practicing their soft skills.

The idea in this paper is that while it is not possible for any curriculum to provide 10,000 hours of hands-on work (Gladwell, 2013), there are other alternatives to labs and simulations to provide opportunities to students to develop their technical as well as soft skills. To integrate depth and breadth, cybersecurity teaching curriculum must indeed emulate real work circumstances, conducted in a dynamic physical learning environment capable of supporting team activity. This, however, is very desirable but sometimes not possible. The idea in this paper is that in order to create deep thinkers and skilled cyber specialist, equipped with the required soft skills, colleges can accommodate students to run their own consulting opportunities in the local community. This approach allows students to be part of a student consulting that provides free services to small business and non-profits. This affords opportunities to students to work with the community as consultants in order to understand a particular community problem or need as it relates to technology or cybersecurity. By consulting, students may acquire a sense of urgency to provide solutions to community problems, strengthen their technical skills and practice the soft skills needed in the profession.

2. Consulting as a Form of Experiential Learning

Consulting, including training and development, needs to be addressed in the cybersecurity curriculum because these skills are growing importance to students in their cybersecurity careers. The profession requires students to have the ability to rapidly adapt as new threats are encountered. That's a key element for cybersecurity graduates – the idea that cybersecurity professionals must constantly push their abilities to predict and stop future threats in a fast-evolving field. All businesses, small or large, depend on the cybersecurity practitioners' ability to innovate, respond and protect. This requires the educational entities to create new methods of educating and training a new generation of cybersecurity experts who must gain many skills to be successful in their career.

Many cybersecurity concepts can be taught in the classroom via labs and simulations but nothing can take place of real world experience where students can interact with actual clients to not only solve real world complex problems but to also gain deeper understanding of important concepts such as human cognition while practicing their soft skills. With consulting skills growing in importance in security field, it is imperative to help students develop those skills and knowledge. Providing consulting experience prepares students for engaging in consulting activities, including research, assessment, training and development, facilitation, and evaluation. Higher education must ensure that students' technical and soft skills

are aligned with the industry needs. One way to do that is by providing students to offer consulting advice to small local businesses under a faculty supervision. Teaching students to apply their knowledge and skills to benefit small businesses is one exceptionally high impact method to foster greater learning experience.

Consulting, as a form of experiential learning, can be incorporated into the cybersecurity curriculum. This will allow educators to wed learning goals and projects involving business security needs to enhance both student workforce readiness and businesses' security readiness. Early involvement of students in consulting can extend their involvement in the field beyond the school and provide deeper knowledge of the discipline. By consulting, students will acquire a sense of urgency to provide solutions to community problems, strengthen their technical skills and practice the soft skills needed in the profession.

Furthermore, the good pay, valuable experience, priceless networking opportunities draw cybersecurity college graduates to employment in consulting which inherently demands students to leverage their knowledge and experience. When students consult with a client, they draw on principles and concepts they have learned in their classes. They are obliged to test their technical and soft skills and apply the underlying lessons they learned during their coursework. A consulting experience for a cybersecurity student has the potential to provide an academic opportunity to test out their training in a safe, structured, and supportive atmosphere before they enter the actual workplace upon graduation. Additionally, real-life consulting opportunities provide students with a better understanding of actual business operations as opposed to traditional approaches.

3. Cybersecurity Education Challenges

Colleges across the country are rapidly creating cyber degree programs and competing to recruit students to this challenging but financially rewarding fields. Yet, there seems to be a growing gap between what graduates learn in school and what the market demands. There are numerous examples in addition to literature support for the notion that cybersecurity education needs to refocus on depth as opposed to breadth (Manson & Pike, 2014). Higher education has not responded adequately to the need of preparing students with a good balance of depth and breadth for this complex environment. There are several challenges which are discussed in this section.

Gap in alignment between education and industry: This challenge is evident in the lack of graduates with sufficient hands-on skill sets to make them ready to perform jobs. But this is a difficult challenge. The cyber security workforce needs are new to most organizations. Defining the needs has been challenging for a number of reasons. First, the digital revolution has been marked by sweeping technology changes. Second, with the rapid advance of new platforms, protocols and business uses, the driving force of advancement has been one of features, not security. Firms roll out new IT solutions for business reasons, and when it comes to resource allocation, the initial push has always been for more features. Security frequently takes a back seat, is seen as a cost, and the developmental resources for security have been scarce. Even if the need is defined, there are additional daunting challenges. According to Conklin, Cline & Roosa (2019), "security, by its very nature, requires a deep understanding not just of the technology, but of security principles as well. This means that the best candidates for security positions

typically have significant technology experience and have many other career options. Growing security personnel from the ground up is a multi-year proposition, as it takes years of experience to develop maturity in the requisite knowledge, skills and abilities to perform many of the complex security tasks". The typical security functions in a modern enterprise include a mix of strategic and tactical operations. From deploying and monitoring security controls, to incident response, analysis, and forensics. The end result is a thorough capability in risk management. In an enterprise with many large scale critical systems, the detailed level of enterprise specific knowledge makes it difficult for someone to cover the entire spectrum of operations. In addition, many organizations claim that today's graduates lack the soft skills needed to succeed in their careers. This issue becomes more critical in cybersecurity field since there is not only a shortage of technical savvy professionals to fill cybersecurity roles but there is also a dearth of cybersecurity job applicants who possess the soft skills, such as strategic planning, change management, and human cognition and behavior (Conklin, Cline & Roosa, 2019).

Depth vs. Breath: Developing capabilities that meet the ever growing and changing demands of the cybersecurity discipline requires a new approach to the process of educating students. Cybersecurity education today begins at college for most students and focuses on breadth. Breadth is appealing as it is primarily concerned with knowledge acquisition, it is easily taught in an instructor-centered model and it can be fit neatly into courses making it ideally suited for a traditional classroom (Katz, 2019).

Depth, on the other hand, focuses on the ability to apply effectively ones knowledge and skills to an authentic real-world problem. Depth cannot fit into a traditional classroom and does not fit into an instructor led approach. Depth can be supported and even inspired in a classroom; however, students must take what they learn and apply it independently (Katz, 2019). 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 own learning to meet current tasks. Learning requirements for depth must be flexible and always expanding keeping pace with industry, learning to deal with last year's cybersecurity challenges is insufficient. Through competition and other mechanisms, students must face current challenges and learn to devise solutions in the face of a changing landscape. In this paper, we recognize depth as a challenge in cybersecurity education and focus on sustainable strategies to provide more depth it applies to cybersecurity skills.

Training vs. Education: Cybersecurity industry expects students to be ready for the field and prepared to work in a team equipped with skills and knowledge with the ability to adapt to change (Conklin, Cline & Roosa, 2019) Cybersecurity education and training can be broadly defined as providing the knowledge and skills to people to carry out the security role in any situation (Department of Homeland Security Excellence, 2014). However, training tends more focused on hands-on technical skills. A good example in cybersecurity area would be to train students to develop and implement specific firewall rules on a Cisco router. As Conklin, and Roosa (2019) put it, education tends to focus on more theoretical ideas behind concepts. They provide good examples by saying that we can teach a student about firewall rules, their strengths and weaknesses, and their application in defending against cyber-threats. The result of education is an understanding of set of concepts, while the outcome of training is a set of skills for using existing tools to solve complex problems (Department of Homeland Security Excellence, 2014)

4. Most Essential Skills for Cybersecurity Professionals

In preparation for the development of a consulting model for undergraduate students, a short interview with 30 security industry leaders working across the United States provided us some input on feasibility of student-led consultancy and emerging security professional skills that can be learned through consulting. The results are summarized in Figure 1 which only show the soft/workplace skills.

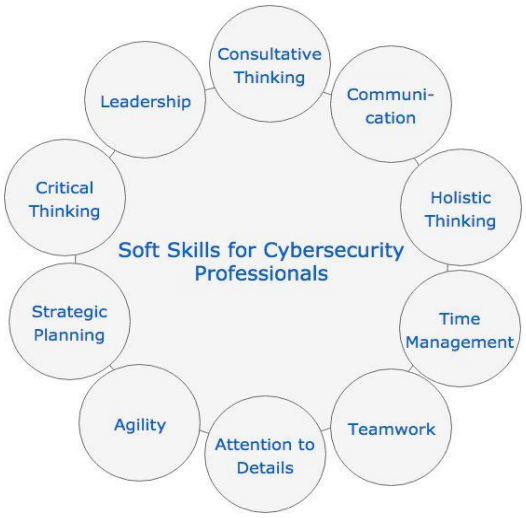


Figure 1. Soft Skills for Cybersecurity Professionals

Consultancy-Thinking: Security Practitioners have to think like a consultant, whether they are advising the company on their security policies, or helping them evaluate the security of the cloud-app they plan to adopt. Cybersecurity experts should be able to look at the big picture and ask the right questions to their team in order to solve real business problems. This is supported by literature that rather than operate at a "purely tactical level, security staff should know how to layout project plans that their efforts can be executed and measured against and understand how their work impacts the organization's bottom-line" [Goodyear, Lichtenberg, Bang, Both & Gregg, 2014; Distilino IT Advisory, 2016).

Time-management training: demands long hours of work under high pressure due to the nature of the profession. There are often tight deadlines to various unexpected issues.

Teamwork: Consulting is often a team project, thus, one of the most important skills a consultant needs is the ability to work well with others which is a critical component to succeed as a cybersecurity practitioner.

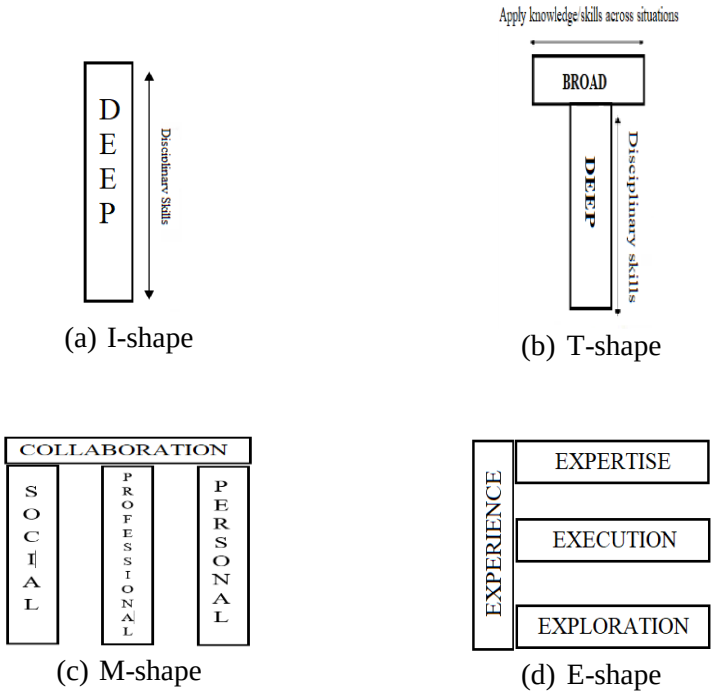
Critical and Holistic Thinking: Effective cyber security specialists must be able to think differently to be able to anticipate and defend against internal and external threats. For example, they should be able to think holistically and critically in specific contexts as well as vague and indeterminate contexts. The literature also supports the notion of students having the ability to analyze complex problems and evaluate options, and the ability to explain the solution and the reasoning behind it (Insight Assessments, 2019; Hoffman, Burley & Toregas, 2011).

Fast Decision-making/Leadership: Through consulting students will learn leadership skills, ability to be innovative with their ideas, and reason in a logical manner. To tackle cyber threats, they will have to make decision on the spot since they will be part of a team that in many occasions might have to reverse a cyber-threat. Through consulting, students learn that they cannot let someone else pick up the slack.

Respondents also mentioned that cybersecurity practitioners have to possess intellectual curiosity and moral responsibility. They should have knowledge of strategic planning, change management, and human cognition and behavior.
They should think like a hacker and an innovator. They should be adaptable and resourceful. They also agreed that more T- and E-shaped workers are needed in the field.

5. E-shaped Security Practitioners

Cybersecurity is inherently and interdisciplinary field. To promote cybersecurity skills, as mentioned in the previous section, recognized as essential for cyber professionals, the "shape" of practitioners, as shown in Figure 2, must also change to adapt to the new cybersecurity workplace.



(a) I-shape (b) T-shape

(c) M-shape (d) E-shape

Figure 2. Types of Professionals

Therefore, a cross section of T-shaped (Figure 2a) and E-shaped (Figure 2d) graduates are required for a true transformation to occur. The new trend in cybersecurity education is to shift talent model to incorporate more T- and E-shaped skill sets, inclusive of integrative problem solvers, automation/development skills sets, in addition to depth in security technologies. Traditionally, there has been an ongoing movement to educate T-shaped students, those with disciplinary depth as well as interdisciplinary breadth. Most curricula, however, compartmentalize the

depth and breadth into different courses. The issue with this model is that current graduates are not T-shaped, but are better characterized as two disjoined lines. In order for students to make the connection, combining T- and E-shapes of teaching and learning must be created in which they can practice joining breadth and depth.

As shown in Figure 2a, I-shaped individuals think narrow and tight and have no breath. They are proficient in a specific area of expertise. On the other hand, T-shaped individuals (Figure 2b) are those who have the depth and breath, which means that they have deep understanding of skills required in their own fields but they are also able to collaborate with people from other disciplines. The key skills for T-shaped professionals are in the areas of "communications, teamwork ability, critical thinking, leadership, empathy, cultural awareness, creativity and innovation" (North, Maier, Haas, 2018). M-shaped individuals (Figure 2c), are equal or more knowledgeable in the skills expected of a T-shaped. M-shaped individuals have more and better skills and competencies than the T-shaped.

E-Shaped (Figure 2d) people have a combination of '4-E's': experience and expertise, exploration and execution. The last two traits, *exploration and execution*, are really necessary in cybersecurity workforce. Table 1 shows a comparison of the different shapes (*Huether, 2019).*

*Table 1. Shape Comparison (*Huether, 2019)

"I-shaped" (Specialist)	"T-shaped" (Generalized-Specialists)	"E-shaped" (NextGen Specialists)
Deep expertise in one area	Deep expertise in one area	Deep **expertise** in a few areas
Very few skills or experience in other areas	Broad skills across several areas	**Experience** across several areas Proven **execution** skills Always **exploring** and innovating
Can creates bottlenecks	Can help remove bottlenecks	Almost limitless potential
Insensitive to downstream waste and impact	Sensitive to downstream waste and impact	
Inhibits planning flexibility or absorption of variability	Improves planning flexible and absorbs variability	

To achieve producing T- and E- shaped individuals, a combination of experiential and integrative learning is needed and can be achieved by consulting activities. Experimental "the knowledge gained through experiences and interactions with the social and learning environment. Integrative learning can be attributed to fostering the ability among learners to make, recognize and evaluate connections among disparate concepts, fields or contexts" (Huber, Brown, Hutchings, Miller, Breen, B, 2007; North, Maier, Haas, 2018). Based on our own experiences and the views of cybersecurity respondents in this study, the technical and operational nature of cybersecurity requires a different teaching and training pedagogy that integrates experience based learning with other integrative learning theories. Cybersecurity practitioners require technical skills sets and experience working with a variety of tools and technologies. But they also need soft skills since the profession requires teamwork, strong communication skills and many other unique skills specific to the field. By providing consulting, students' learning experience is centered on the real-world context which will promote critical thinking and problem solving approaches (Birenbaum, Breuer, Cascallar, Dochy, Dori, Ridgway, 2006; Abraham & Shih, 2015). Integrative learning approaches

include analyzing real-world problems through different viewpoints and considering different solutions to problem. Cybersecurity is a practice oriented discipline and requires critical thinking skills and the ability to analyze a situation through multiple perspectives (Bishop & Irivine, 2010; Abraham & Shih, 2015).

By combining approaches from both learning theories we will be able to produce T- and E-shaped graduates who are equipped with "breadth" and "depth", as well as the execution and exploration skills, implying having both a big-picture outlook and an attention to detail which are important components of being a cybersecurity practitioner. In this case, we have the potential of preparing T-shaped individuals for becoming E-shaped professionals as they gain more work experience. In Agile environments such as cybersecurity, there is need for T- or E-shaped professionals. T-shaped professionals have a depth of experience in one technical specialty and have a good working knowledge in other areas. E-shaped Professionals, on the other hand, have deep expertise in several domains. Since cybersecurity education is a new and evolving field of study, it presents new opportunities for curriculum reform in higher education to reshape teaching strategies to develop T-shaped individuals with the potential of becoming E-shaped employees who not only have valuable technical knowledge/skills but they are also able to communicate their ideas, solve complex problems, think like a hacker and work well in teams, among many other skills. Such reform is very critical for higher education institutions as cybersecurity demands are growing rapidly.

6. Benefits of Student-Led Consultancy

Training cybersecurity students is similar to training a pilot, an athlete or a doctor (Manson & Pike (2014). Time spent on the task for which the person is being prepared is critical for success. The common theme between all of the analogies for cybersecurity education is that they represent a set of complex tasks that require a high degree of mastery to gain success (Manson & Pike (2014). Learning to be agile, making decisions fast, coping with long work hours, solving complex problems, working collaboratively, and thinking like a hacker are becoming few of the essential skills in cybersecurity. All these soft skills are necessary but difficult or sometimes nearly impossible to teach in the classroom or even labs. An important piece of any training is the opportunity to work in a real-world environment to ensure that the students gain a good understanding of technical skills. However, as mentioned before in this paper, to align with the needs of organizations, students not only need the technical skills but they also need to be exposed to real world situations in which they can also practice their soft skills. They need to be a combination of T- and E- shaped professionals. The area of consulting, including training and development, is proposed in this paper as the means for meeting this need. The relevance of consulting to cybersecurity is evident because of the predominance of career opportunities in this profession. Through student-led consulting, students will (1) engage in practical exploration of the consulting field, investigating what consulting entails generally and the range of options available for students choosing to pursue consulting-related work in cybersecurity, (2) engage in solving complex security for small businesses and organizations, and (3) practice skills necessary to succeed in the field of cybersecurity.

Many small business and non-profit organizations need consulting services but do not have the financial resources to pay consulting fees. This creates a great opportunity for students since such businesses are often open to bringing in trainee consultants, such as students. This will also small businesses the opportunity to bringing expert advice without the monetary costs. By using student consultants, these organizations can help develop a new generation of skilled workers to increase workforce pipeline and economic growth. Students, in turn, get to experience most phases of the project working in teams, as opposed to an internship situation, where a student may find working alone as a less rewarding experience in terms of personal development (Troper & Lopez, 2009).

The idea of a student-led consultancy firm is to challenge students beyond their academic curriculum by working on real life consulting projects. This will give an opportunity to students to apply their theoretical knowledge in real world situations while gaining practical work experience. In this case each student has the opportunity to take meaningful responsibility to shape the organization's future. Students can also develop skills which go beyond their own field of studies through trainings and their interaction with the clients. Consulting offers businesses research and information that empowers them, while providing students with hands-on experiential learning that is much more valuable than a classroom case study.

7. Student-Led Consultancy Model

The model proposed in this paper is a multilayered approach based on Nyquist and Wulff's model (2001), shown in Figure 3. Nyquist and Wulff (2001) approach consulting from a research perspective. They introduce the notion that by utilizing this particular model students learn to think about consulting as a systematic process of data collection and analysis. They also see consulting as a research-based activity that requires critical thinking and problem solving skills. For example, they learn that the process of organizational assessment requires them to gather information in order to assess the problem accurately. They must select appropriate data gathering tools and then must engage in data analysis and interpretation. They must not only be able to identify themes and patterns but to figure out what those patterns mean. Finally, Students must be able to determine how best to address the results of their needs assessment research (Nyquist and Wulff's, 2001).

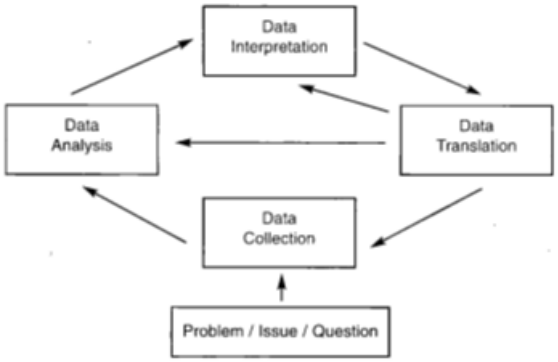


Figure 3. Nyquist and Wulff's model (2001)

We strongly believe that consulting skills can be and should be taught in a regular classroom. And students should be able to practice their skills in real work

environments. Also, based on our observation, many small businesses and non-profit organizations need consulting services but do not have the financial resources to pay consulting fees. This creates a great opportunity for students since such businesses are often open to bringing in trainee consultants, such as students. This will also give small businesses the opportunity to bring expert advice without the monetary costs. Our proposed idea is based on Nyquist and Wulff's model in that for semester-long projects, we ask students to assume the role of a consultant. We team up students, faculty and employers to develop a project, integrating research-based activities to help students gain technical and employability skills. In the context of cybersecurity, we teach students "to think beyond their fields and collaborate to develop, accept, and implement holistic, integrated solutions to complex security problems" (Hoffman, Burley & Toregas, 2011). Then we prepare students to approach local businesses to offer free consulting in cybersecurity. This approach includes not only teaching the concepts and skills to students via labs and simulations but also offering practical skills via consulting which will offer a different experience than internships. Through this experience, students "get to experience most phases of the project with the social support of a team including their faculty supervisor, as opposed to an internship situation, where a student may find working alone as a less rewarding experience in terms of personal development (Troper & Lopez, 2009)".

As a pilot for this study, a group of students worked side-by side by a faculty supervisor partnering with a K-12 school client to solve their most difficult challenges through a combination of consulting, analytics, cybersecurity, and innovation expertise. Their role in the project was to analyze the existing systems and recommend integrated security system solutions that would ensure proprietary or confidential data and systems are protected. Students found that of the key aspects of cybersecurity is the Human, which is notion supported by research. Therefore, the proposed developing material for computer security education or awareness programs for school employees. Students were able to identify few issues such that at times, student networks are not completely separate from staff and administrative networks. Free wifi around the school buildings and students using the wifi provides thousands of opportunities for hackers to gain access to a school network, especially when students download free, infected apps on their phones. It only takes a click on one email infected with malware to collect login information from a system administrator who has access to the networks to breach an entire school system. Many schools do not have the budget to hire a bigger cybersecurity team and pay for necessary resources, such as software and replacing old operating systems to protect school networks. Students offered some foundational practices that school districts must employ to protect student and staff data. These practices include offloading as much data as possible to reputable vendors to increase data protection and safety; implementing strict network segregation to ensure that students do not have access to staff, administrator, and administrative systems; making sure that students, staff, and administration are aware of phishing, ransomware, and related attacks; implementing a routine vulnerability scanning and remediation schedule that also prioritizes the latest vulnerabilities and risks; and having an incident response plan in place and exercised for when bad things happen. Such plan may include procedures for how to contact local law enforcement. Student consultants want to continue working with the schools to see what can and should be done to raise the bar on cybersecurity practices, despite constrained budgets. They are trying to find ways to focus on fundamental practices without breaking the bank.

According to students, strict network segregation coupled with an awareness program, vulnerability management capability, and other basic security hygiene practices can help make schools a harder target for hackers. Creating opportunities for students to act as consultants offered them the chance to review security policy, re-write the policies if needed, create strategic planning, and detect, identify and respond to existing threats under the supervision of a faculty or a designated security practitioner.

Through consulting under the faculty supervision, students can develop strong cybersecurity as well as soft, considering that organizations desperately need to keep up with the evolving threat landscape. With this approach, students can have hands-on experiences needed to prepare them for future opportunities. By working together with the local businesses, higher education can ensure that students come out of cybersecurity programs armed with breadth and depth of cybersecurity issues to tackle complex problems and threats in the security landscape. They will also have the required skills to become agile problem solvers, holistic thinkers and fast decision makers with great time management skills.

8. Conclusions

Acknowledging that much remains to be done for the idea in this paper to come to fruition, our work generates important call for the need for a multifaceted approach to Cybersecurity education that draws on consulting experience. The value and need for focusing on depth in cybersecurity education is clear. Students should have the opportunity to work in meaningful environments and be in control of their own learning, attaining firsthand experience with the real world. This will allow students to develop mastery and industry preparedness helping them to hit the ground running and to provide significant contributions right out of college. The six to eight year employee training noted by many industry leaders will be greatly reduced to training just for the unique attributes of specific companies and industries. A student-run consulting will empower students to provide services to small business and non-profits. This allows students to work with the community as consultants in order to understand particular community problems or needs as they relate to technology and cybersecurity. This will also allow faculty to prepare T- and E-shaped students to meet the fast-growing demands in cybersecurity workforce. The good pay, valuable experience, priceless networking opportunities draw cybersecurity college graduates to employment in consulting which inherently demands students to leverage their knowledge and experience. When students consult with a client, they draw on principles and concepts they have learned in their classes. They are obliged to test their technical and soft skills and apply the underlying lessons they learned during their coursework. A consulting experience for a cybersecurity student has the potential to provide an academic opportunity to test out their training in a safe, structured, and supportive atmosphere before they enter the actual workplace upon graduation. Additionally, real-life consulting opportunities provide students with a better understanding of actual business operations as opposed to traditional approaches.

References

Abraham, S. & Shih, L. (2015). Instructional Perspective: Towards an Integrative Learning Approach in Cybersecurity Education, *Information Secuirty Education Journal*, 2(2), 84-90.

Assante, M. J., & Tobey, D. H. (2011). Enhancing the Cybersecurity Workforce. *IT Professional,* 13(1), 12-15. doi:10.1109/mitp.2011.6

Birenbaum, M., Breuer, K., Cascallar, E., Dochy, F., Dori, Y., Ridgway, J., et al. (2006). A learning integrated assessment system. *Educational Research Review* 1(1), 61-67.

Bishop, M. and Irivine, C. (2010). Demystifying Cybersecurity. *IEEE Computer and Reliable Societies.* May/June 2010.

Conklin, W., Cline, R., & Roosa, T. (2019). Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors. Retrieved from https://www.semanticscholar.org/paper/Re-engineering-Cybersecurity-Education-in-the-US%3A-Conklin-Cline/d38d8286ee93c5351d80a9bba05df6bc3e0f5c61

Department of Homeland Security Excellence (2014). Report on Cyber Security Education Project, Retrieved from https://ccicada.org/wp-content/uploads/2015/03/CyberSecurityEducationReport_CCICADA_6-9-14Final.pdf?cv=1

Distilinfo IT Advisory (2016). Five soft skills Young cybersecurity professionals need to get ahead. Retrieved from https://www.distilnfo.com/itadvisory/2016/06/15/5-soft-skills-young-cybersecurity-professionals-need-to-get-ahead/?cv=1

Gladwell, M. (2013). *Outliers*. New York: Back Bay Books.

Goodyear, R., Lichtenberg, J., W., Bang, K., Both Gregg, J. (2014). Ten Changes Psychotherapists Typically Make as They Mature Into the Role of Supervisor, 70(11), Wiley Publishing.

Hoffman, L., Burley, D., Toregas, C. (2011). Holistically Building the Cybersecurity Workforce, *IEEE Security & Privacy*, 10(2), 22-39.

Huber, M. T., Brown, C., Hutchings, P., Gale, R., Miller, R., Breen, B. (Eds.). (2007). Integrative Learning: Opportunities to Connect. Association of American Colleges and Universities and the Carnegie Foundation for the Advancement of Teaching.

Huether, D. (2019). Break Organizational Dependencies with an E-shaped Staff. Retrieved from https://www.leadingagile.com/2017/02/e-shaped-staff/

Informationweek.com. (2019). [Online] Available at: http://www.informationweek.com/pdf_whitepapers/approved/1407550418_2014_Ponemon_Cost_of_Data_Breach_Study.pdf [Accessed 8 Apr. 2019].

Insight Assessment (2019). Cybersecurity starts with critical thinking. Retrieved from: https://chs.insightassessment.com/Uses/Client-Solutions/Cyber-Security-Starts-With-Critical-Thinking?cv=1

Javidi, G., Sheybani, E. (2018). K-12 Cybersecurity Education, Research, and Outreach. *2018 IEEE Frontiers in Education Conference*, October 2018.

Katz. (2019). Breadth vs. Depth: Best Practices Teaching Cybersecurity in a Small Public University Sharing Models. Retrieved from https://www.jstor.org/stable/e26491216

Lee, J., Bagchi-Sen, S., Rao, H. R., & Upadhyaya, S. J. (2010). Anatomy of the Information Security Workforce. *IT Professional,* 12(1), 14-23. doi:10.1109/mitp.2010.23

Manson, D., & Pike, R. (2014). The case for depth in cybersecurity education. *ACM Inroads*, 5(1), 47-52. doi: 10.1145/2568195.2568212

North, K., Maier, R., Haas, O. (2018). Knowledge Management in Digital Change: New Findings and Practical Cases, Springer International Publishing.

Nyquist, J. D., & Wulff, D. H. (2001). Consulting using a research perspective. In K. G. Lewis & J. Povlacs Lunde (Eds.). Face to face: A sourcebook of individual techniques for faculty/instructional developers (2nd ed., pp. 45-62). Stillwater, OK: New Forums Press.

Robinson, D., Lloyd Sherwood, A., & DePaolo, C. (2009). Service-Learning by Doing. *Journal of Management Education*, 34(1), 88-112. doi: 10.1177/1052562909339025

Troper, J., & Lopez, P. (2009). Empowering novice consultants: New ideas and structured approaches for consulting projects. *Consulting Psychology Journal: Practice and Research*, 61(4), 335-352. doi: 10.1037/a0017843