National Cybersecurity Institute Journal

Volume 3, No. 2

ISSN 2333-7184

National Cybersecurity Institute | 2000 M Street, Suite 500 | Washington, D.C. 20036
Excelsior College | 7 Columbia Circle | Albany, NY 12203-5159

NATIONAL CYBERSECURITY INSTITUTE JOURNAL

Volume 3, No. 2

EDITORIAL BOARD

PEER REVIEWERS

The *National Cybersecurity Institute Journal* gratefully acknowledges the reviewers who have provided valuable service to the work of the journal:

NATIONAL CYBERSECURITY INSTITUTE JOURNAL

The National Cybersecurity Institute at Excelsior College is a research center based in Washington, DC, dedicated to increasing knowledge of the cybersecurity discipline and its workforce demands. Published three times a year, the peer-reviewed National Cybersecurity Institute Journal covers topics that appeal to a broad readership within the cybersecurity discipline, with a particular focus on education, training, and workforce development.

The manuscripts submitted to the journal are reviewed for their contribution to the advancement of applied research in the area of cybersecurity.

Submission guidelines for authors can be found at http://ncij.excelsior.edu/.

FROM THE EDITOR

Greetings and welcome to the second issue in Volume 3 of the National Cybersecurity Institute Journal. As those with a vested interest in cybersecurity are aware, there is a paucity of well-educated and trained individuals to meet the demand for cybersecurity professionals. Numerous efforts to reduce the gap in the cyber workforce are underway, including finding ways to increase the number of women and minorities in the field. Community colleges play an important role in that effort, and in this issue of our journal we will examine some of those efforts through the perspective of five notable authors. With each issue of this journal we will continue to increase awareness and knowledge of the various aspects of the cybersecurity discipline to help everyone better understand and meet the escalating challenges in the cyber community.

In our first article, Charles Parker presents us with "Cybersecurity Gender Inequality: The Role and Effort of the Community College," a paper that provides an overview of the status of women in the cyber workforce and what community colleges, acting as a gateway to knowledge, are doing to increase the participation of women in IT. Next, the team of Benito R. Fernández, Carlos A. García, José R. Capriles, Wendy Ford, and Christine Mooney provide us with their paper, "Building Bridges: From NSF ICorps to Community Colleges—Cybersecurity for All," which highlights how The University of Texas at Austin and Queensborough Community College are collaborating to increase the engagement of traditionally underrepresented people in the cybersecurity workforce. In his offering, "Meeting the Present and Future Demands of Cybersecurity," Kevin Lemmon provides an overview of government actions such as Executive Order 13587 that seeks to recruit and retain cyber professionals, and how groups such as Women in Technology (WIT) are working to recruit increasing numbers of women into the cyber arena. Next, in "2 Plus 2 Cybersecurity Education—Transfer Pathways for Women and Minorities," authors Laila Khreisat and Neelu Sinha discuss in detail how Fairleigh Dickinson University's Community College Partnership Program has brought both bachelor's and master's degrees to underrepresented regions of New Jersey. In so doing it has created a much-needed pipeline of diverse cybersecurity individuals, by providing transfer students with varying opportunities to pursue degrees in the cyber field. Finally, from the great state of Hawaii, Debra A. Nakama at the University of Hawaii Maui College offers us "Community College's Outreach Role in Cybersecurity." This article emphasizes the importance of an outreach program in expanding access to careers in the cybersecurity field with particular emphasis on the inclusion of women and minorities to improve their economic security.

The editors at the NCI Journal believe these articles relating to the efforts of community colleges across the nation to increase participation in cybersecurity will educate our readers and provide them with useful information that can be applied to their own systems and organizations to strengthen their systems cybersecurity.

Cybersecurity is of prime importance to businesses and their stakeholders, and to the countless individuals who operate a digital system. At the NCI Journal we work continually to publish articles that you, our readers, will find helpful both to you personally and to the benefit of your organization. Many thanks go to all the contributors, administration, and staff for their ongoing efforts to bring this latest edition of the National Cybersecurity Institute Journal to fruition. I look forward to your comments, suggestions, and future submissions to the journal.

Jane LeClair

Jane A. LeClair, EdD
Editor in Chief and Founder, National Cybersecurity Institute

Cybersecurity Gender Inequality: The Role and Effort of the Community College

Charles Parker II, PhD

INTRODUCTION

The information technology (IT) field finds itself intertwined with both consumers and business operations on a variety of levels. Consumers are most familiar with using laptops, desktops, scanners, and the Internet as they participate in their daily activities. Meanwhile, businesses use laptops, desktops, the Internet, and server farms with rows of racks, cables, and a dazzling array of indicator lights as they exchange information with customers and others in the marketplace. One facet equally important to both consumers and businesses alike is cybersecurity. At a superficial level, consumers might be familiar with cybersecurity due to the antivirus programs they have purchased year after year or through the occasional pop-up advertisement recommending that their systems be scanned or updated. Businesses, on the other hand, also use antivirus software alongside web content filtering and other tools. Both business entities and consumers have to secure the data on their respective systems. In the case of businesses, owners or C-suite personnel are responsible for ensuring that there are appropriate measures incorporated into the business's cybersecurity operations to mitigate any risks of breaches.

As simple a task as this appears, accomplishing this has proven to be exceptionally difficult. This is evidenced by the prevalence of malware infections, systems being used as bots, and similar breaches occurring within businesses. Often, these breaches are published rather frequently as they occur. The target of such attacks may have their records encrypted by the attackers, a type of attack known as ransomware. In these cases, the business would depend on back up files being current or—worst case scenario—pay some level of fee.

A recent example of a business's data being encrypted by a third-party in the headlines is when Hollywood Presbyterian Medical Hospital had to pay the equivalent of $17,000 in bitcoin for the decryption key to their data (Winton, 2016; Whiteside & Yeo, 2016). Had the hospital had a structured cybersecurity plan in place and followed their back-up policy, the victim may not have had to pay the ransom fee or the loss of their data may not have been as serious. If the attacker desired, the records or data could be sold on the dark web instead—an option for the attacker if they refused to work with the business and collect the ransom from them. This was recently demonstrated as an attacker sold a total of 9.3 million patient records from an unknown medical facility (Mearian, 2016). If the business is not careful and has not learned from its errors or remediated its vulnerabilities, the business may be breached more than once. This occurred with the Hard Rock Café in Las Vegas when it was breached a second time (Ragan, 2016), as announced on May 13, 2016.

The department tasked with defending against these types of attacks has commonly been known as the Information Security or Information Security and Privacy department. The staff members are tasked with protecting and securing the business enterprise and its data from all attackers. These deviants can be located anywhere on the globe and may attack the business day or night from a business's Internet connectivity. The attacks may be simple intrusions, re-attempted attacks from previous years, or slight variations of existing attacks. The department responsible for protecting the business may vary in size based on the size of the business, its needs, and the risks the business has.

STATEMENT OF THE PROBLEM

The cybersecurity challenge has grown in relevance and scope. Although IT departments are staffed by both men and women, historically, there has been a low participation within IT—and by extension, cybersecurity—of women. This is not a new phenomenon and is not a peculiarity to the U.S., but has been seen in other countries, including Kenya (Muthama, Kimathi, & Kitung'u, 2013) and in Wales, U.K. (Dallaway, 2013). Various measures have been attempted to remediate this issue, including affirmative action (Muthama, Kimathi, & Kitung'u, 2013). These methods have not worked well as evidenced by the lack of progress and continued disparity between the genders. Steps taken to address the problem up to this point have been rather ineffectual.

DISPARITY

The distribution within the IT field between the two genders is rather glaring. As a point of comparison, just fewer than 33% of doctors and 35% of lawyers in the U.S. are women. However, only up to 10% of women work in information security (Wolff, 2015; Morgan, 2016). Other research indicated that 26% of the science, technology, engineering, and math (STEM) staff members were women, and only 11% of staff worked in cybersecurity (Nelson, 2015). The research undoubtedly indicates there are significantly fewer women working in the IT field—particularly in cybersecurity. Had prior programs designed to elevate the number of women in cybersecurity worked, these numbers would be much higher.

There is a huge demand for expertise in this field and industry. This is a function of the amount of work in IT and the amount of risk involved with systems. As a result, there is a great opportunity due to the labor supply shortage (Morgan, 2016). Clearly, business needs to focus more on gender diversity.

To improve the distribution to a more equitable level, action is required. At minimum, with a greater balance of diversity in place, the cybersecurity field would significantly improve (Stapf & Hall, 2016). This paradigm shift is difficult to administer at the career level. A male-dominated infrastructure is already in place and has existed for years. One potential solution could be for senior management to issue a directive stating that diversity would need to change (i.e., improve) in the next 1.5 years. However, this approach is problematic in that the business may fill positions with staff not entirely qualified to meet the demands of the role in order to simply meet the numbers. There are better ways to address the issue.

Another possible point of contact to assist with this issue would be the community colleges. Community colleges have the opportunity to be the gateway for education for students interested in the cybersecurity field. These facilities allow for the students to learn a trade, matriculate to the associate degree, and continue on if they have a desire to complete a bachelor's degree. However, the community colleges also have a similar challenge to address.

The American Association of University Women (2013) researched this disparity issue. For the school year 2009-2010 in IT there were 3,359 associate degrees earned by women as compared to 10,860 by men. This shows that over three times more men earned an associate degree in computers and information sciences as compared to women during the same period. This offers the community colleges the opportunity to not only work on issues within an educational context, but also to provide an improved level of gender mix to the information sciences and cybersecurity field. The community colleges provide the avenue for women to become involved in IT—particularly cybersecurity.

LACK OF TARGETED RESEARCH

Community colleges provide a valuable service to students and have the opportunity to influence women and deliver information on careers within the cybersecurity field. Because students are on campus or logging in from other locations for online courses, the potential to offer the information is far-reaching.

The efforts taken by community colleges in encourage women to enter the cybersecurity track—and subsequently the cybersecurity industry—have not been significantly researched. When compared to the other fields taught at the community college level, this field of study is relatively new. In addition, this field is constantly changing as it relates to attacks, defenses, and other facets of cybersecurity which further complicates the process of creating a curriculum.

LITERARY REVIEW

The literature focused on women already working in the field, partnerships, and cybersecurity teachers. One of the first research projects regarding women in cybersecurity focused on the ratio of women in cybersecurity (Bagchi-Sen, Rao, Upadhyaya, and Chai, 2010). Historically, dating back to 2006, only 13% of the cybersecurity workforce consisted of women. Researchers noted the industry needed to encourage women to work in cybersecurity. The study sampled women who were chief security officers and chief information officers within their respective companies. This was a rather small group of 33. The research indicated there were two main barriers experienced early in the women's careers: 1) training and 2) work environment. With respect to training, the two main factors inhibiting women's careers were not knowing how to apply technology in real-world experiences and a lack of exposure working within a team. The study found that women's career advancement was limited by the level of skill, the work environment in transferring from a technical to a management position, and personal reasons related to their work-family balance. The required technical skills were relatively clear. The other needed skills were vague and subjective.

Manson, Curl, and Carlin (2012) researched partnerships between universities and high schools. This partnership focused on the CyberPatriot competition. This was designed to increase the number of people working in cybersecurity. There has been a distinct shortage of persons with degrees in the STEM fields of study.

Pusey and Sadera (2011) researched programs for educating teachers. The research focused on the teacher's level of understanding and their self-perceived ability to teach the subjects. The sample of 318 pre-service teachers asked them to self-rate on cyber-ethics, cyber-safety, and cybersecurity. The research indicated the respondents were not prepared to model or teach these subjects. The respondents noted they could model or teach 4% of the topics as they were presented with.

COMMUNITY COLLEGES

The community colleges have a unique and pertinent role to play. This was noted at the Community College Cyber Summit (3CS) (Dohm, 2015). These institutions have the ability to provide an education to some who may not normally have this opportunity. This may be due to the generally lower cost, the community college being located closer to the student's home, the parents wanting their child to attend at a smaller institution prior to transferring to a larger institution, or the student and/or parents not wanting a mass amount of debt for the first two years of education.

As community colleges enroll students, and during the student's time matriculating, colleges have the opportunity to expose cybersecurity to new and returning students. This may be a new field for them to understand since they may have only read about it or heard about this field on the news or elsewhere in the media. This is an opportunity to inform them and provide information on the program and prospects for a career.

Because there is a significant disparity between the numbers of men and women working in IT and cybersecurity-related fields, the matriculation period also allows the community college system the opportunity to bring more awareness to women about this industry.

The community colleges, to assist with this mission, may partner with organizations in the community (Dastmozd, n.d.) to help increase the level of knowledge within the community and generate interest in the cybersecurity field among women. The option for the industry to partner with the schools (Carnelley, 2016) is a good fit. The industry knows the skills needed for the person to be successful in the role and has the funds to assist with the programs. This amount may not be significant; however, it certainly would help. The industry also may have the necessary influence to help initiate change. In certain environments, the process may take an extended period of time. With a business in the industry leveraging their own influence, it may reduce the time to necessary to disseminate the information and make adjustments into the curriculum.

The community college, in order to attract more women into the cybersecurity field, may also sponsor or host events showcasing cybersecurity, its future, careers, applications, and other facets of the industry. One method may be to hold a hackathon (Wolff, 2015). Historically, there has not been a large number or ratio of women attending these. Community colleges may provide an environment to encourage women to attend and participate. Once women attend such events and see how very interesting and promising this field is, there may be more interest.

There may also be conferences held that focus on women in cybersecurity. As an example, the Second Annual Women in Cybersecurity conference was held from March 27-28, 2015 in Atlanta, GA (Nelson, 2015). These conferences would also serve as a mechanism to draw women in and listen to speakers on cybersecurity topics in an environment where industry professionals are present and can provide their business information and possibly collect résumés for positions and internships.

Community colleges also have the opportunity to partner with one or more of the several organizations focused on increasing the number of women in cybersecurity (National Initiative for Cybersecurity Careers and Studies (NICCS), 2015). The NICCS notes several institutions and groups whose mission it is to support and encourage women to work in cybersecurity. These were varied in their focus, and include the Anita Borg Institute and Anita Borg Institute's Grace Hopper Celebration of Women in Computing, focusing on helping women improve their career and contribute significantly to technical fields. Additionally, the Women in Cyber Security initiative was designed to recruit, retain, and advance the careers of women in cybersecurity. The Women's Society of Cyberjutsu (WSC) has a mission of empowering women in the cybersecurity field. The Women's Symposium for Cyber Security is a goal-oriented organization aimed at improving the number of women in cybersecurity via informing women about resources, networking opportunities, and mentors. The National Cybersecurity Institute (NCI) at Excelsior College's Initiative for Women in Cybersecurity (IWICS) provides webinars, podcasts, and articles for women as encouragement. Lastly, the SANS Cyber Talent Immersion Academy for Women also provides training and certification programs for women.

As women continue to explore courses and various topics, these efforts may work as another tool to provide information on careers in IT and cybersecurity. These efforts have not been studied at length and may have more of an influence on the individuals presently pursuing this course of study and later their careers.

COMMUNITY COLLEGE INFORMATION SECURITY PROGRAMS

For community colleges to assist in training and educating women in cybersecurity, there would need to be programs available at these community colleges in the cybersecurity field of study. There are currently a number of these across the U.S., including, but not limited to, Tidewater Community College, Rockland Community College, Monroe Community College, Hagerstown Community College, Northern Virginia Community College, Howard Community College, Anne Arundel Community College, Honolulu Community College, Houston Community College, Mohawk Valley Community College, and Carroll Community College.

CONCLUSION

The efforts expended by community colleges to teach students in the field of IT in general—and more specifically, cybersecurity—need to be studied at length. There are a number of community colleges across the U.S. that offer specific programs to this end, while other programs may be used for more of a background in this specific sub-field. Community colleges have the distinct opportunity to be a driving force in improving the current gender disparity in cybersecurity. There are also ample resources to assist them in this process.

Other than the programs and coursework being noted in a community college's course bulletin, there has not been an abundance of research performed on the topic. Although this is exceptionally vital to business and consumers, there is still a shortage of staff members overall, and particularly women in this field. This is an opportunity for community colleges to become a more active participant in resolving this issue.

REFERENCES CITED

Bagchi-Sen, S., Rao, H.R., Upadhyaya, S.J., and Chai, S. (2010). Women in cybersecurity: A study of career advancement. *IT Professional Magazine*, 12(1), 24–31. doi:http://dx.doi.org/10.1109/MITP.2010.39

Carnelley, D. (2016, June 29). How the cybersecurity skills gap is being closed. Retrieved from https://securityintelligence.com/how-the-cybersecurity-skills-gap-is-being-closed/

Dallaway, E. (2013, October 17). Let's hear it for the ladies: Women in information. Retrieved from http://www.infosecurity-magazine-features/lets-hear-it-for-the-ladies-women/

Dastmozd, R. (n.d.). Community colleges play more vital role than ever. Retrieved from http://www.huffingtonpost.com/rassoul-dastmodz-phd/community-colleges-play-m_b_4723295.html

Dohm, L. (2015, January 27). Community College Cyber Summit (3CS) Addresses the Need for Cybersecurity Education ASAP. Retrieved from http://www.prweb.com/releases/communitycollegecyber/2015summit/prweb12472719.htm

Loricchio, L. (2015, August 22). Carroll community college to launch cybersecurity program. Retrieved from http://www.carrollcountytimes.com/news/local/ph-cc-cybersecurity-program-20150822-story.html

Manson, D., Curl, S., and Carlin, A. (2012). CyberPatriot: Exploring university-high school partnerships. *Communications of the IIMA*, 12(1), 65–77.

Mearian, L. (2016, June 28). Update: Hacker puts 9.3M U.S. patient records up for sale. Retrieved from http://www.computerworld.com/article/3088963/healthcare-IT/hacker-puts-650k-u-s-patient-records-up-for-sale.html

Morgan, S. (2016, March 28). Calling all women: The cybersecurity field needs you and there's a millions jobs waiting. Retrieved from http://www.forbes.com/sites/stevemorgan/2016/03/28/calling-all0women-the-cybersecurity-field-needs-you/#35f01835ca4c

Muthama, M.N., Kimathi, K.P., and Kitung'u, K.M. (2013). Gender issues in information technology. *International Journal of Mechanical Engineering Research & Applications*, 1(3), 1–7. Retrieved from www.ijmera.org and http://www.academia.edu/4255475/Gender_issues_in_Information_Technology

National Initiative for Cybersecurity Careers and Studies. (2015, December 17). Women & minorities: The need for women and minorities in cybersecurity. Retrieved from https://niccs.us-cert.gov/home/women-minorities

Nelson, K. (2015, March 16). Gender differences could be a boon to cybersecurity industry. Retrieved from http://www.washingtonexaminer.com/gender-differences-could-be-a-boon-to-cybersecurity-industry/article/2561464

Pusey, P., & Sadera, W.A. (2011). Cyberethics, cybersafety, and cybersecurity: Preservice teacher education to make a difference. *Journal of Digital Learning in Teacher Education*, 28(2), 82–88.

Ragan, S. (2016, June 28). Hard Rock Las Vegas suffers a second data breach. Retrieved from http://www.csoonline.com/article/3089449/security/hard-rock-las-vegas-suffers-a-second-data-breach.html

St. Rose, A., & Hill, C. (2013). Women in community colleges: Access to success. Washington, D.C.: AAUW. Retrieved from http://www.aauw.org/files/2013/05/women-in-community-colleges.pdf

Stapf, E., & Hall, S. (2016, March 7). Advancing the ranks of women in cybersecurity. Retrieved from http://usblogs.pwc.com/cyberseucrity/advancing-the-ranks-of-women-in-cybersecurity/

Whiteside, Jr., L., & Yeo, M.L. (2016, February 24). Hollywood Presbyterian: Is this only the beginning? Retrieved from http://knowledge.wharton.upenn.edu/article/whitehside-yeo-hollywood-presby-ransomware/

Winton, R. (2016, February 18). Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating. Retrieved from http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

Wolff, J. (2015, November 11). Hackathons have a gender problem. Retrieved from http://www.slate.com/articles/technology/future_tense/2015/11/why_don_t_more_women_work_in_cybersecurity.html

AUTHOR

Charles Parker II, PhD (ABD), is an information security analyst. He has worked in the automotive, healthcare, and banking industries. Parker received the MSA, MBA, JD and LLM, and is completing his dissertation on ICS/SCADA insecurity in the wastewater treatment facility industry. His research focuses on SCADA, AV, cryptography, langsec, and vehicle insecurities.

Building Bridges: From NSF I-Corps to Community Colleges — Cybersecurity for All

Benito R. Fernández, PhD | Carlos A. García, BS | José R. Capriles, MS
Wendy Ford, PhD | Christine Mooney, Esq.

ABSTRACT

Cybersecurity is a very real problem in our society. Although there is a wealth of information about it available in a multitude of places, the information does not reach those who are most vulnerable. New threats continue to challenge information security professionals; however, tools exist that can reduce the risk to the majority of the population. What is needed is an effective mechanism to disseminate up-to-date information to the stakeholders in a timely manner. We believe that community colleges offer a unique opportunity to be the catalyst to such an endeavor. This paper provides concrete examples of the manner in which faculty at The University of Texas at Austin (UTA) and Queensborough Community College (QCC) collaborated to assess how the STOP.THINK. CONNECT. (2016) model can be implemented at community colleges. The article will focus on the development of the relationship, aspects of the model, reflections on the cross-disciplinary outcomes, and results as a means for others to increase the engagement of underrepresented populations in the cybersecurity workforce.

INTRODUCTION

At the present, the term cybersecurity is on everyone's mind. In fact, it's no longer merely a technical expression introduced by corporations trying to describe a problem. It's totally the opposite. Corporations, governments, and regular citizens are keenly aware of the existence of cyber-attacks involving data loss, identity theft, virus, and malware, among others. Unfortunately, not everyone has access to best practices and solutions that could help them mitigate or avoid problems. Cybersecurity is a monster that not everybody is willing to confront. However—like David and Goliath—in most of the cases, they just need the right tool to stand up to a bigger adversary.

During the last decade, the world has seen news about cyber-attacks with more frequency than in previous decades. In these different attacks, cars were hacked, WikiLeaks disclosed private information, the accounts of famous people were hacked, financial information was stolen, and even a nuclear plant was hacked. A CBS (2015) article entitled, "These Cybercrime Statistics Will Make You Think Twice About Your Password: Where's the CSI Cyber team when you need them?" poses the question: *think cyber-crime is something only found in fiction?* Their study found that online crime is a very real threat in our Internet-connected society. With 1.5 million annual cyber-attacks, online crime is a real threat to anyone on the Internet. That number means there are over 4,000 cyber-attacks every day, 170 attacks every hour, or nearly three attacks every minute. The same report states that in 2014, 47% of American adults had their personal information stolen by hackers (Pagliery, 2014)—primarily through data breaches at large companies. "The absolute size of the breaches is increasing," said Michael Bruemmer, vice president of the credit information company Experian's data breach resolution group, which sponsored the report. Despite the rise in breaches, 27% of companies did not have a data breach response plan or team in place, though that is down from 39% in the previous year's survey. Bruemmer also said that 15% of the breaches are not reported.

As mentioned in the February 2013 (White House, 2013) Executive Order to improve critical infrastructure cybersecurity, "Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats." During the Global Conference on Cyberspace (2013) held in Seoul, the cyberspace was globally recognized as international critical infrastructure. The international community commitment to Open and Secure Cyberspace resulted in the Seoul Framework (2013) created at the Global Conference on CyberSpace (2015) which stated, "The global and open nature of the Internet is a driving force in accelerating progress towards development in its various forms." The framework also mentioned, "Governments, business, organizations, and individual owners and users of information technologies (cyberspace) must assume responsibility for and take steps to enhance the security of the information technologies. States and relevant regional and international organizations that have developed strategies to deal with cybersecurity and the protection of critical information infrastructures are encouraged to share their practices and measures that could assist other Member States in their efforts to facilitate the achievement of cybersecurity."

In 2014, the National Institute of Standards and Technology, or NIST (June 2016), with help from the private sector, released a Cybersecurity Framework to address the executive order. Over the last years the framework has been adopted as a standard for the industry. "The Framework is voluntary guidance, based on existing standards, guidelines, and practices, for critical infrastructure organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders" (NIST, June 2016). In 2015, during the Global Conference in Cyberspace held in the Netherlands, the governments of the world ratified the importance of international cooperation in order to confront daily challenges related to cybersecurity. Moreover, the conference promoted that one of the key elements to addressing those challenges is cybersecurity education. In fact, more security professionals are needed today and even more will be required in the future. If we want to be prepared to face every single cyber threat in a more efficient way, we need to foster innovation inside all academic institutions. We need to increase students' awareness and motivate them to discover solutions or create new ones. Educators and professionals must promote their participation in the global community to increase technological innovation.

It is crystal clear that even small improvements in cybersecurity could potentially benefit the entire society. Collectively, we discovered that just a few small steps have the ability to open tremendous opportunities for our students and colleagues. We decided to apply the premise of divide and conquer. This paper focuses on a successful collaboration between The University of Texas at Austin (UTA) and Queensborough Community College (QCC) to better serve their stakeholders by helping students and their parents or children increase their knowledge about cybersecurity.

BACKGROUND

ABOUT STOP.THINK.CONNECT.

In 2010, President Barack Obama designated October as National Cybersecurity Awareness Month. It also marked the launch of the national campaign known, as "STOP.THINK.CONNECT., a unique partnership between public and private entities aimed at increasing cybersecurity awareness throughout the country. The STOP.THINK.CONNECT. campaign, spearheaded by the Department of Homeland Security (DHS), focuses on promoting the importance and awareness of cybersecurity education. The slogan is indicative of the call to action that must be echoed at every community college throughout the United States, which enrolls more than 46% of the nation's undergraduate students (AACC Fast Facts, 2015). In addition to DHS, leadership for the STOP.THINK.CONNECT. campaign is also provided by the National Cyber Security Alliance (NCSA) and the Anti-Phishing Working Group (APWG). The campaign's website provides a plethora of available resources for organizations and individuals to use in educating others about cybersecurity awareness.

The noteworthy goals of this campaign speak to the importance of linkages that should exist among community colleges, industry, and other institutions of higher education. Some of the goals of STOP.THINK.CONNECT. are as follows:

A. Increase and reinforce awareness of cybersecurity, including associated risks and threats, and provide solutions for increasing cybersecurity.

B. Communicate approaches and strategies for the public to keep themselves, their families and their communities safer online.

C. Increase the number of national stakeholders and community-based organizations engaged in educating the public about cybersecurity and what people can do to protect themselves online. (STOP.THINK.CONNECT., 2016).

ROLE FOR EDUCATORS

The STOP.THINK.CONNECT. goals provide unique opportunities for community college educators to engage in the dialogue about increasing the level of knowledge and training available in the realm of cybersecurity. More importantly, the campaign brings to the forefront the importance of an interdisciplinary need to begin the discussion about cybersecurity awareness, education, and training. Knowledge about cybersecurity can be effectively promoted through a three-pronged approach that includes awareness, education, and training.

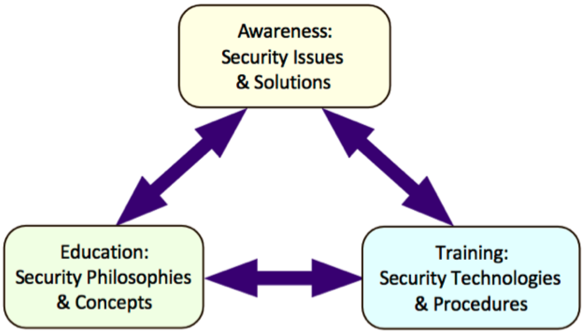


Figure 1. Cybersecurity Knowledge Loop. *The arrows between the three types of knowledge indicate that each area supports and informs the other areas. Any change in the knowledge acquired in each area can trigger a cascaded response in the others. When one is aware of the issues related to cybersecurity, a context for understanding cybersecurity concepts is developed. Likewise, training in cybersecurity technology provides insights into known solutions and potential issues. The open nature of the cybersecurity knowledge loop suggests that cybersecurity learning can begin with awareness, education, or training and people can and will move among the three different areas depending on their circumstances and needs.*

Woerner (2012) distinguishes the characteristics of the three different cybersecurity knowledge areas in relation to purpose and duration (See Figure 1). Awareness is designed to increase high-level knowledge or consciousness about cybersecurity issues. This is an ongoing process of varying duration. People can engage in cybersecurity awareness activities over as little as a day or up to over several weeks. Awareness is also an ongoing continual activity as cybersecurity issues change and evolve. Educators can engage people of all ages in awareness activities as a valuable way to encourage safe and responsible cybersecurity actions. For example, this includes learning about keeping digital devices safe from hackers and protecting personal information online.

Cybersecurity training seeks to address tactical and operational knowledge gaps by building explicit skills used to solve problems. Training can usually be done in short durations that last for a few weeks or months at a time. This is when hands-on tools and virtual learning environments play a key role in allowing learners to experience—in real-time—the impact of cyber-attacks in a safe setting, practice how to solve cybersecurity problems, and discover solution pathways. Community colleges are uniquely qualified to provide cybersecurity training to high school students through innovative early college high school programs, to recent high school graduates who are seeking skills that will rapidly prepare them for the 21st century workforce, to 4-year college students that can take college credits at a lower cost, and to displaced or repositioned workers who may be in need of re-training to remain competitive in today's economic environment. Entry level training includes configuring and maintaining networks, computer programming, basic computer hardware, and operating system installation and monitoring.

Finally, cybersecurity education provides the philosophical and conceptual context for the security tools, techniques, technologies, and procedures that are fundamental to cybersecurity. Education provides an opportunity for critical thinking about and strategic analysis of issues related to the implications and outlook for cybersecurity. This may include exploring policy as it relates to cyber challenges or understanding how to incorporate cybersecurity concepts into strategic goals. Cyber education is an ongoing process that may take months or years, depending on specific goals and objectives, and is valuable in a post-secondary setting as well as in corporate and organizational training arenas.

Thus, awareness, training, and education address the "what," the "how," and the "why" of cybersecurity knowledge. In practice however, the distinctions between cybersecurity awareness, training, and education may often overlap. Nevertheless, the goals are the same: to educate the populace about the risks inherent in cyber networks, to empower everyone to make smart decisions to protect themselves, their families, and employers online and to protect their digital (private and proprietary) data, and to energize and train a competent workforce to support the needs of business, industry, and our local, state, and federal governments.

Educational institutions can support cybersecurity awareness and education in a variety of ways. For example, they can elect to participate in the STOP. THINK.CONNECT. campaign. Academic Alliance is a nationwide network of nonprofit colleges and universities committed to promoting safer online practices. These colleges, along with others, are updating their curriculums and programs to incorporate cyber education and promote cyber awareness through their websites and through campus-wide seminars. Additionally, these colleges are partnering with local public and private agencies to enhance their cyber education capacity (Estrella Mountain Community College, 2016; Aims Community College, 2016).

In addition, the STOP.THINK.CONNECT. campaign can be a launching point for a wide variety of innovative opportunities for faculty members from all disciplines to incorporate cybersecurity education in their course offerings. For example, the DHS website provides free resources that can be used for educating students about account authentication, tip sheets, and an online safety quiz. One specific resource offered is the Digital Bliss tip sheet. The sheet was used by a faculty member in a marketing class to educate community college students about client interaction, security, and privacy concerns. Cybersecurity is not a topic that is generally covered in an Introduction to Marketing course. However, due to the resources made available through the STOP.THINK. CONNECT. campaign, the faculty member was able to use this as a tool to inform students about being responsible digital citizens in their personal and professional lives. One of the major challenges facing educators is the need to understand that cybersecurity is "for all"—not just for computer science or computer information systems faculty and students. The need for increased awareness and understanding is echoed in the statistics from the United States Bureau of Labor Statistics (BLS).

According to BLS, more than half of the occupations projected to grow over the next seven years require some form of post-secondary education. Jobs that require the attainment of postsecondary education provide higher wages for employees. Positions that require some information security analyst training are expected to grow at a rate of eighteen percent between 2014 and 2024 (Woerner, 2012). These statistics speak to the importance of workforce opportunities for community college students in the coming years. More than 46% of undergraduate students in the United States are enrolled at community colleges. (AACC, Fast Facts, 2015). Therefore, the role of community colleges in providing access to cybersecurity and comprehensive postsecondary education has grown. More importantly, community colleges must align themselves with four-year institutions who specialize in discovery and outreach in the field of cybersecurity to ensure access to proper resources.

AN OPPORTUNITY

According to the 2014 Census on Educational Attainment (U.S. Census Bureau, 2014), 67 million out of 209 million Americans over age 25 have a bachelor's degree or higher. That means that about 68% of them do not have a bachelor's degree. The proportion of high school graduates that go to college has been declining over the last few years (Floyd, 2014). According to the National Center for Educational Statistics (NCES 2015), of the over 20 million students that are expected to attend American colleges and universities, about 7 million will attend a 2-year institution (NCES, 2014b). According to the Bureau of Labor Statistics (Bureau of Labor Statistics, 2016), during the 2015–2016 academic year, colleges and universities are expected to award nearly 1 million associate degrees; 1.8 million bachelor's degrees; 800,00 thousand master's degrees; and 200,000 doctoral degrees. So close to a third of the undergraduates go through the community colleges (NCES, 2014a).

According to the Program for International Student Assessment (PISA) report (NCES, 2014c), 15-year-old students in the United States had an average score of 498, which puts the U.S. in the middle of the pack. Twelve education systems had higher scores, eight had lower than average scores, and 11 had average scores similar to the U.S. The Organization for Economic Co-operation and Development, or OECD (OECD, 2016) average score was 497. For adults, the numbers are similar. According to the OECD report (NCES, 2014d) on the Program for International Assessment of Adult Competencies (PIAAC), the average literacy score for adults ages 16–65 ranged between 250 and 269. The U.S. average score was 272, which was not significantly different than the PIAAC average score. There were seven countries higher, six lower, and eight similar. In numeracy, the range was 246–288, with the U.S. at 257; 16 countries were higher, three lower, and two similar. And finally in problem solving (in technology-rich environments), the range was 274–294. The U.S. had the lowest score with only one other country posting similar average scores. There were 16 countries above. Given the overwhelming evidence, targeting community and technical colleges is the fastest way to reach a large segment of the labor force.

The 2012 Information Technology Workforce Assessment for Cybersecurity (ITWAC) from DHS (Department of Homeland Security, 2012), found that only 59% of their civilian workforce satisfies their information assurance (IA) compliance. A new study finds that 1 in 10 people who regularly use a computer or other digital device to connect to the Internet have received some kind of cyber security training in the last 12 months, and more than two thirds have never had any such training. Indeed, a shocking 68 percent say they have never had any such training—ever (WeLiveSecurity, 2012). These and other findings were revealed by ESET (2016) at the Virus Bulletin conference in Dallas. Another ESET poll was conducted by Harris early in 2016. The purpose of that poll was to study implications of the *bring-your-own-device* or BYOD trend (90% of Americans own a computerized gadget (Gahran, 2011)). They asked employed U.S. adults if they had received any kind of computer security training from their employer and only 32 percent said they had (WeLiveSecurity, 2012).

It would seem obvious that cyber education is a priority and we need to target the K-12 population and their families. We need to get them involved. There is an abundance of information available in the web related to cybersecurity (Greenlight, 2015; Olstik, 2015) but most people are not aware of the seriousness of the problem and whether they might be a target. As an example of an opportunity, the Center for Identity (2016) at The University of Texas has an educational program (Center for Identity, 2016c) that includes free games for children *Beat the Thief* (Center for Identity, 2016b). The game's curricula (Center for Identity, 2016d) mentions that 96% of teens use social networking applications such as Facebook, MySpace, chat rooms, and blogs (GuardChild, 2016). Children are targeted for identity theft 35 times more often than adults (AllClearID, 2016). To help education this vulnerable population, we could target state educational policies that should require sixth graders to comply with a proficiency test in cybersecurity. Courses should be certified, online, and free for everyone. We need to create a discipline in children—one that will continue through adulthood—on how to be cyber safe! We propose that one of the most effective ways to increase cybersecurity awareness and workforce opportunities is to build bridges.

BUILDING BRIDGES AND CONNECTIONS AMONG EDUCATORS AND CS PROFESSIONALS

The expanding role of community colleges as centers for workforce and economic development is illustrative of the need to build bridges. Faculty at community colleges face heavy teaching loads, insufficient professional development resources, and increasing challenges with changing technology. The need to build bridges for shared curriculum and professional development resources between two and four year institutions is critical. "The programs and supports offered by community colleges are often lacking in coherence and supports" (Jenkins & Cho, 2013). Jenkins and Cho also suggest that the integration of programs and support systems will provide for a higher degree of support for students. In addition to integrated support systems for students, they propose a new approach to professional development for faculty.

Traditional professional development activity programs for faculty focus on the teaching style of the individual faculty member. Professional conferences often consist of professional development workshops or panel discussions. Faculty must be provided the opportunity to build cross-disciplinary bridges among themselves. Community college faculty professional development should include a focus on time for collaborative development amongst faculty to create guided pathways (Jenkins & Cho, 2013). The cross-disciplinary bridge that has been established between the team at the University of Texas at Austin and Queensborough Community College serves as a model pathway that other institutions can develop.

OUR JOURNEY—I-CORPS LEARNINGS

WHAT IS THE I-CORPS PROGRAM?

The National Science Foundation I-Corps (NSF I-Corps) program began in 2011. The main goal of the program is to provide critical training to assist in the commercialization of engineering and scientific technologies into viable and innovation businesses (NSF, 2016). The program is an intensive seven-week training program facilitated by in-person and WebEx training sessions. A team—comprised of three members—may apply to the NSF for selection as a participant in the program and consists of (1) an Entrepreneurial Lead (EL), a graduate or postdoctoral student, (2) an Industry Mentor (IM), and (3) a Principal Investigator (PI), typically a faculty researcher. The program provides training for researchers using the Lean LaunchPad methodology of teaching a hypothesis-based testing pedagogy (Pellicane & Blaho, 2014). The team begins their journey at a three-day in-person training event focused on training around the various aspects of the Business Model Canvas.

Teams are required to present an initial hypothesis, also known as their value proposition. Over the next several weeks the teams engage in conducting research through "customer discovery". Known as "get out of the building," this unique training focuses on the team on listening to the pains of their potential customers. It is not a process aimed at teaching the team to sell their product, but instead to discover the needs of their customer. An important aspect of the process is listening. Teams are required to conduct a minimum of one hundred (100) customer discovery interviews during the seven-week period. These interviews are aimed at assisting the team in assessing whether there is a product market fit for their research. Over the seven weeks, the teams hold office hours with the teaching team through Skype and WebEx sessions. The team's program and weekly insights are tracked through an online platform known as LaunchPad Central.

UT AUSTIN—JOURNEY—WHY I-CORPS?

UT's involvement in the I-Corps program germinated out of an internal project by Dr. Benito Fernandez related to an application of his patented technology[1] (hybrid computing) to encryption sponsored by UT's Center for Identity (CID). The CID's mission is to deliver the highest-quality discoveries, applications, education, and outreach for excellence in identity management, privacy, and security. Dr. Fernandez and his team had participated in many CID events over the years and witnessing what industry needed, they started to work in an application that will make communication secure and private. Under the auspices of CID, researchers under Dr. Fernandez's leadership developed tools for a secure cyber-infrastructure communication system. The technology developed includes a hybrid (mixed-signal: analog and digital) processor that can be used as a pseudo-random number generator (PRNG). The generator creates an "infinite key" using chaotic oscillator dynamics—this means that our encryption is a One-Time-Pad (OTP), an encryption key as long as the message itself (the most secure form of encryption). In conjunction with the PRNG, the UT team also developed an algorithm to encrypt/decrypt messages on-the-fly with almost no overhead—an important requirement given the large volume of communication over the Internet. After a patent was filed with the Office of Technology Commercialization (OTC), the UT team applied to the NSF's I-Corps program to further increase its outreach and validate the need for such a product.

The team was assigned the New York City Regional Innovation Node (NYCRIN) with Executive Director Dr. John A. Blaho, also Director of CUNY Industrial-Academic Research. During I-Corps, the team was advised by several coaches from diverse backgrounds. One of the coaches was Professor Christine Mooney from Queensborough Community College, City University of New York (QCC-CUNY). Her invaluable assistance in business and legal matters helped the UT team to broaden their focus and through her contacts, the team was able to connect with professionals in the cybersecurity industry. In particular, Professor Mooney and the team spoke with prominent speakers who are industry members of the National Initiative for Cybersecurity Education (NICE, 2016) working groups. During the interview process (customer discovery phase in I-Corps), we realized that a major barrier for industry professionals is the lack of "valid" knowledge about cybersecurity.

A large number of the interviewees lacked proper or up-to-date knowledge of the current state of cybersecurity. For example, with Professor Mooney's assistance,

[1] Patents # US 0117083: Apparatus for solving differential equations, # US 7454450: Mixed-signal system for performing Taylor series function approximation, and # US 7796075: Method and apparatus for internally calibrating mixed-signal devices.

a plan began to be formulated on how to use community colleges as a beachfront to implement an outreach mechanism to a large sector of the population. Eventually encompassing the K-12 population and their parents, 2- and 4-year college students and through them, their families.

It became readily apparent from the customer discovery process that the I-Corps team was not the only one engaging in a listening exercise, but instead the team and the faculty member were building valuable bridges for both.

I-CORPS LEARNING

The I-Corps program selects a team with at least three member personas: a Principal Investigator (PI), Benito R. Fernández, an Entrepreneurial Lead (EL), José R. Capriles, and a Business Mentor (BM), Carlos A. García. Each team member has a different set of responsibilities.

NSF Innovation Corps seeks to prepare scientists and engineers for entrepreneurship. The learning methodology is based in the build-measure-learn feedback loop under the guidance of established entrepreneurs. A key element of this program is determining the problem that needs to be solved and then developing a minimum viable product (MVP) to begin the learning process as quickly as possible. In the course, every decision made by each team is understood to be a hypothesis that needs to be validated via a designed experiment. The experiments are performed in the field (by getting out of the office/lab) with potential customers, clients, suppliers, etc. One of the first lessons learned for many of the teams was that startups are not a small version of a corporation. Usually in a manufacturing business, customers don't care how the product is assembled, only that it works correctly. But in a startup this is not the case; who the customer is and what the customer might find valuable are usually unknown and this is the reason why the hypothesis validation process is so important.

The idea is to achieve as much validated learning as quickly as possible. This way the teams can establish facts about validity of the vision and if it is sustainable. The hypothesis validation is achieved by talking directly with the possible customer—known as customer discovery. The instructor trains the members of the teams on how to perform market validation-type interviews and pushes the members of the teams to go out of the building. This is essential for the value proposition development of the startup. Even when experiments produce a negative result, those failures are used to make a structural course correction—or pivot—that creates a new fundamental hypothesis about the product, market, strategy, etc. and represents the engine of growth. This is proved to be instructive and can influence the strategy of the startup. Another critical aspect is that the inventors are the ones most qualified to perform customer discovery. The main idea here is that it is the inventor, not a hired marketing specialist, who can decide what may need to be changed in the product specifications, functionality, etc.—decisions which can only be addressed during the interview.

BUILDING BRIDGES FOR COMMUNITY COLLEGES

Community colleges, by design, build bridges within the communities they serve, for the people they educate, and the lives that they transform. Since the 1950s, community colleges have provided roles of community service, community development, and economic development (Jenkins & Cho, 2013). Today, the role of the community college is keenly important in developing a highly-skilled 21st century workforce to tackle the problems of business and society (Jenkins & Cho, 2013). One important bridge that community college programs have with the economic community is that of the advisory board.

According to a recent study by Kaupins and Coco (2002) of 114 business school programs that are accredited by the Association of Collegiate Business Schools and Programs (ACBSP), the advisory board's main role is analyzing curriculum issues and developing ideas for new programs. Advisory boards also provide faculty members with advice regarding business trends and community relationships and they support students by serving as guest speakers and providing internships. Queensborough Community College is also accredited by the ACBSP. The Queensborough Community College Advisory Board provides similar types of services as advisory boards as those represented in the study. The Advisory Board consists of eight members representing local businesses, economic development organizations, technology companies, governmental agencies, and financial institutions. The Business Department faculty, which offers degree programs in the areas of business administration, accounting, management, computer information systems, and office administration and technology, meets annually with the advisory board to review the curriculums and discuss industry trends. In addition, our advisory board members have actively supported our students by participating in service-learning events and engaging in business research and classroom projects.

When community colleges seek to build bridges with the community, the business advisory board is a logical starting place. The QCC Business Advisory Board takes their responsibilities very seriously and has not only initiated changes in our curriculum, but has also supported faculty members as they implemented changes by providing letters of support for grant initiatives. The University of Texas faculty engaged in this I-Corps project attended one of the QCC Business Advisory Board meetings and also provided curriculum support and guidance. This level of support from external partners helps to ensure that community college programs remain relevant and that community college students have the workplace knowledge and skills that employers value.

QUEENSBOROUGH COMMUNITY COLLEGE—TAKEAWAYS FROM I-CORPS TEAM PARTICIPATION

One of the most important opportunities for faculty is the chance to network and share best practices with their peers. This type of sharing provides invaluable time for people to learn, redefine, and improve their existing pedagogical practices. Unfortunately, for community college faculty, these encounters are limited. Most institutions provide limited funds for faculty to travel and attend conferences. In addition, the registration costs and day-to-day responsibilities prevent many faculty from attending these professional development conferences.

In January of 2016, Professor Christine Mooney, a member of the Business Department at QCC-CUNY was able to serve as a member of the teaching team for the New York City Regional Innovation Node (NYCRIN) national cohort. The faculty member was able to interact with I-Corps teams from different regions throughout the United States. As members of the teaching team, faculty are encouraged to interact and assist the participants. Prof. Mooney was encouraged to assist the team from The University of Texas at Austin as they began working on a cybersecurity project. The subject matter of their research was of interest to her as an attorney, but more importantly, as an instructor of business law. The topic of cybersecurity law is a rapidly expanding field, and one which is highly specialized. The team began to work with the adjunct faculty member from QCC-CUNY over the next seven weeks. Together they embarked on a customer discovery journey. One of the goals for the UT Austin team was to conduct customer discovery interviews about their proposed cybersecurity project. This led the community college faculty member engaging in research about resources and programs around cybersecurity.

It very quickly became apparent that the research was producing results for both the UT Austin team and QCC-CUNY. Over the next several months, the UT Austin team became members of the Business Department Advisory board and began to share technology resources and programs with the community college faculty. The interactions facilitated a greater awareness about cybersecurity resources, programs, and other avenues available to community college students and faculty. For example, the collaborative research resulted in the discovery of the National Initiative for Cybersecurity Education (NICE) led by the National Institute of Standards and Technology (NIST). NICE (2016) provides unique opportunities for members of academia, industry, and government entities to openly discuss initiatives, programs, and events aimed at promoting cybersecurity education. NICE also provides several working groups aimed at addressing unique populations. The NICE K-12 working group is an amazing resource of data and program materials. Over the last several months, the community college faculty have joined this working group and acquired key programmatic information to assist in curriculum development. Furthermore, the working group provides updates about programs around the country that give working group members access to a plethora of resources. This discovery would not have been made without the bridge developed between the UT Austin and QCC faculty teams.

The involvement of the team in the Business Advisory Board functions and programmatic design for faculty was invaluable. Another unanticipated outcome of the bridge building was the interface between the community college students and the team. The City University of New York (CUNY) hosts an annual Community College Innovation Challenge for students. The program utilizes a modified I-Corps curriculum that engages students in a similar training program. This year, the community college students were paired with the team from UT Austin. UT Austin was invaluable in providing mentorship, support, and feedback for the students. The students remarked that the ability to interact with external cybersecurity experts provided key learning opportunities. For example, a student team remarked that he was unaware the Department of Homeland Security proscribed varying levels of encryption for cybersecurity platforms. This discovery led to a change in the focus of his research project. This type of bridge building provides unlimited paths for community college students to develop an awareness of the complexity of cybersecurity.

Other important considerations in community college education for cybersecurity that need to be addressed include faculty development, scaling to effectively meet workforce demands, and training methods. There is a lack of funding for faculty development in this area (Locasto, Ghosh, Jajodia & Stavrou, 2011). Faculty development is needed and sustained funding should be provided to ensure that faculty have the expertise and knowledge to educate students in this area as well as the technology and resources needed (Namin, Hewett & Inan, 2015). In addition, students are not adequately trained to meet workforce needs due to traditional educational methods that lack the resources to train large numbers of cybersecurity specialists. There are many faculty members who do a very good job educating within their classrooms to small batches of students; however, these efforts need to be scaled up to reach a wider audience (Locasto, Ghosh, Jajodia & Stavrou, 2011). Finally, more hands-on training, which increases student enthusiasm, reduces classroom boredom, and allows students to achieve deeper levels of learning, should be included in curriculums (Locasto, Ghosh, Jajodia & Stavrou, 2011) (Giannakas, Kambourakis, Papasalouros & Gritzalis, 2016). Innovative teaching methods, such as digital games, virtual labs, and mobile platforms should be used to engage students. One of the benefits of these modified teaching methods is that community colleges that utilize these methods can reach out to K-12 community partners and provide security awareness training to various levels of students, with a goal of exposing young people to the many career opportunities available within security. Plans for training cybersecurity workers should focus on educating a new workforce rather than mass certification of existing workers (Locasto, Ghosh, Jajodia & Stavrou, 2011).

NEXT STEPS—WHERE DO WE GO FROM HERE?

The lessons learned that have been detailed above can be replicated at other community colleges to help fill the outstanding need for cybersecurity workers and to increase community awareness about cyber safety. The NSF I-Corps Nodes are located throughout the various parts of the country. The opportunity for community colleges to partner with these nodes and share resources is unlimited. The I-Corps teams can provide valuable mentorship and experiential learning opportunities for community college students. In particular, the growing demand for students who have completed an internship or experiential learning opportunity has expanded. This type of bridge building could provide unlimited and unexpected outcomes. The model of cross-institutional bridge building is necessitated by the need for increased cybersecurity awareness and the need for a diverse understanding of business practices.

In September of 2015 MIT and Boston Law School announced a unique partnership that would allow students at MIT to utilize the services of students from Boston Law School for assistance with the legal aspects of their business or innovations. These collaborative relationships speak to the importance of providing cross-disciplinary and cross-institutional relationships. The launch of the Technology & Cyberlaw Clinic at MIT and Boston University Law School is an excellent example of the innovative and necessary partnerships that need to evolve. Community colleges need to begin to align themselves with other institutions to leverage the greatest degree of resources and information for their students.

In addition we propose four additional areas where efforts by community colleges could make a great impact towards increasing interest in cyber safety and cyber careers: 1) Strengthen the educational pipeline from K-12 to 2-year college to 4-year college, 2) Replicate cybersecurity outcomes through multi-faceted awareness projects, 3) Advocate through public-private partnerships, and 4) Measure results. Following are suggested activities in each of these four areas that provide an opportunity for faculty and students to dig deeper into the cybersecurity discipline.

Strengthen the educational pipeline from K-12 to 2-year college to 4-year college

A. I-Corps as a bridge to disseminate innovation to K-12 community and beyond.

Replicate cybersecurity outcomes through multifaceted awareness projects

B. Create cyber awareness web pages with links to helpful resources

C. Develop cybersecurity webinars for targeted audiences to make people aware of the problems and the available solutions

D. Partner with community leaders to develop a marketing plan to bring awareness to the most vulnerable in the community—parents, working adults, children, and senior citizens

E. Organize a meet-up in the local community

F. Offer free cybersecurity awareness courses at the community college

Advocate through public-private partnerships

G. Urge city and state officials to create cybersecurity policies and offer to help promote those policies that already exist

H. Urge local K-12 schools, community colleges, and universities to create cybersecurity policies and offer to help promote those policies that already exist

I. Urge local companies to create cybersecurity policies

J. Partner with the local Small Business Administration (SBA) office or SCORE (Service Corps of Retired Executives) to provide cybersecurity training

Measuring results

K. Write proposals (NSF, etc.) to develop and test these ideas

i. Select a group of individuals in the community

ii. Test their cybersecurity knowledge

iii. Provide information about cybersecurity

iv. Provide tools for them to "*pay it forward!*"

v. Conduct surveys in the community before and after the program to estimate impact in the community

vi. At community colleges, develop executive directive to integrate cybersecurity in the classroom

By following these examples we can achieve cybersecurity for all and community colleges will begin to see bridges that extend far beyond geographic boundaries. The process must be intentional on the part of administrators at the various schools. It is as simple as, "STOP.THINK.CONNECT."

CONCLUSION

This paper presented how bridges can be built between universities and community colleges. We recount how using NSF's Innovation Program: I-Corps—after customer discovery—revealed that most Americans are not aware of the seriousness and pervasiveness of cybersecurity attacks and breaches. Based on this finding, an idea was formulated to attack the problem.

The paper also reviews the state of cybersecurity as it relates to how information reaches the community at large. Since community colleges have built bridges with their neighbors, we propose to use them as the catalyzer for the dissemination of information related to cybersecurity. The approach should be multifaceted and raise awareness of the importance of cybersecurity for everyone—youths through seasoned seniors, and promote the best use and practice of cybersecurity measures, and advocate policies through public-private partnerships.

ACKNOWLEDGMENTS

The UT team would like to acknowledge the National Science Foundation funding under grant #1239136 and the I-Corps Program for funding under grant #1620866. This research was partially funded by the Center for Identity at The University of Texas under contract #CID-2015006. The QCC-CUNY team would like to acknowledge the New York City Regional Innovation Node (NYCRIN) and its National Science Foundation funding under grant #1305023.

REFERENCES CITED

Aims Community College. (2016). Aims and Weld County team up for employer symposium. Retrieved from www.aims.edu/about/departments/marketing/news.php?id=63

AllClearID. (2016). 2012 Research report. Retrieved from https://www.allclearid.com/plans/child/2012research/

American Association of Community Colleges. (2015). Community College Fast Facts. January: AACC, 2013.

Bureau of Labor Statistics. (June 2016). *Occupational outlook handbook*, 201617 edition. U.S. Department of Labor, Information Security Analysts. Retrieved from http://www.bls.gov/ooh/computerandinformationtechnology/informationsecurityanalysts.Htm

CBS. (2015). These cybercrime statistics will make you think twice about your password: Where's the CSI cyber team when you need them?

Retrieved from http://www.cbs.com/shows/csicyber/news/1003888/thesecybercrimestatisticswillmakeyouthinktwiceaboutyour-passwordwheresthecsicyberteamwhenyouneedthem/

Center for Identity (2016). The University of Texas at Austin. Retrieved from https://identity.utexas.edu

Center for Identity. (2016b). Beat the thief game. The University of Texas at Austin. Retrieved from https://identity.utexas.edu/beatthethiefgame

Center for Identity. (2016c). Children's education programs. The University of Texas at Austin. Retrieved from https://identity.utexas.edu/childrenseducationprograms

Center for Identity. (2016d). Beat the thief curriculum. The University of Texas at Austin. Retrieved from https://identity.utexas.edu/assets/archived/Beat%20the%20Thief%20Curriculum.pdf

Department of Homeland Security. (2012). Retrieved from https://cio.gov/wpcontent/uploads/downloads/2013/04/ITWACSummaryReport_04012013.pdf

ESET. (2016). Retrieved from http://www.eset.com/

Estrella Mountain Community College. (2016). AZ energy consortium launches cybersecurity degree. Retrieved from https://news.estrellamountain.edu/2014/08/26/azenergyconsortiumlaunchescybersecuritydegree

Gahran, A. (2011). Report: 90% of Americans own a computerized gadget. CNN. Retrieved from http://www.cnn.com/2011/TECH/mobile/02/03/texting.photos.gahran/

Gahran, A. (2011). Report: 90% of Americans own a computerized gadget. CNN. Retrieved from http://www.cnn.com/2011/TECH/mobile/02/03/texting.photos.gahran/

Giannakas, F., Kambourakis, G., Papasalouros, A., & Gritzalis, S. (2016). Security education and awareness for K6 going mobile. *International Journal of Interactive Mobile Technologies*, 10 (2), 4148.

Global Conference on CyberSpace. (April 2015). Retrieved from https://www.gccs2015.com/seoul1718october2013

Global Conference on CyberSpace. (October 2013). Retrieved from https://www.gccs2015.com/seoul1718october2013

Greenlight Technologies (n.d.). Proactively monitor cyber-attacks and network security. Predict cybersecurity threats and cyber security challenges. Prevent loss and translate the impact of risk with an integrated platform. Retrieved from http://pages.greenlightcorp.com/CyberGovernanceDemo_RequestaCyberGovernanceDemoAW.html?gclid=Cj0KEQjwYO7BRDwi6Stp7T296ABEiQAD6iWMaCLk9duXU7HShs14ssje_FKGnUr36WsBZ96uk7a3N8aAqGr8P8HAQ

Jenkins, D., & Cho, S. (2013). Get with the program ... and finish it: Building guided pathways to accelerate student completion. *New Directions for Community Colleges*, 2013 (164), 2735.doi:10.1002/cc.20078

Kaupins, G., & Coco, M. (2002). Administrator perceptions of business school advisory boards. Education, 123 (2), 351357.

Locasto, M. E., Ghosh, A. K., Jajodia, S., & Stavrou, A. (2011). The ephemeral legion: producing an expert cybersecurity workforce from thin air. Communications of the ACM, 54 (1), 129131.

OECD. (2016). Computer viruses and other malicious software. *Organization for Economic Cooperation and Development*. Retrieved from http://www.keepeek.com/DigitalAssetManagement/oecd/scienceandtechnology/computervirusesandothermalicioussoftware_9789264056510en#page1

Namin, A. S., Hewett, R., & Inan, F. A. (2015). Faculty development programs on cybersecurity for community colleges: An experience and lessons learned report from a two-year education project. *Proceedings of the International Conference on Computer Science Education Innovation & Technology (CSEIT)*, Global Science and Technology Forum. Retrieved from http://crawl.prod.proquest.com.s3.amazonaws.com/fpcache/e31efd6f2b7e7ef242ed103ddc14f40c.pdf?AWSAccessKeyId=AKIAJF7V7KNV2KKY2NUQ&Expires=1466716487&Signature=ylpkgzqPbsNiN9eqv6HxFV5g5EI%3D

NCES. (2015). Fast facts: What are the new back to school statistics for 2015? National Center for Education Statistics. Retrieved from http://nces.ed.gov/fastfacts/display.asp?id=372

NCES. (2014a). Enrollment in elementary, secondary, and degree-granting postsecondary institutions, by level and control of institution, enrollment level, and attendance status and sex of student: Selected years, fall 1990 through fall 2024. National Center for Education Statistics. Retrieved from http://nces.ed.gov/programs/digest/d14/tables/dt14_105.20.asp?current=yes

NCES. (2014b). Degrees conferred by postsecondary institutions, by level of degree and sex of student: Selected years. National Center for Education Statistics, 186970 through 202425. Retrieved from http://nces.ed.gov/programs/digest/d14/tables/dt14_318.10.asp

NCES. (2014c). Selected findings from PISA 2012. National Center for Education Statistics. Retrieved from http://nces.ed.gov/surveys/pisa/pisa2012/pisa2012highlights_1.asp

NCES. (2014d). PIAAC 2012/2014 results. National Center for Education Statistics, 186970 through 202425. Retrieved from http://nces.ed.gov/surveys/piaac/results/summary.aspx

NICE. (2016). The National Initiative for Cybersecurity Education (NICE). Retrieved from http://csrc.nist.gov/nice/about/index.html

NIST. (June 2016). Retrieved from http://www.nist.gov/

Norris, F. (2014). Fewer U.S. graduates opt for college after high school. *New York Times*. Retrieved from http://www.nytimes.com/2014/04/26/business/fewerushighschoolgraduatesoptforcollege.html?_r=1

NSF. (2016). Retrieved from http://www.nsf.gov/news/special_reports/i-corps/about.jsp.

Oltsik, J. (May 2015). An analytics-based approach to cybersecurity. Enterprise Strategy Group. Retrieved from https://www.splunk.com/content/dam/splunk2/pdfs/whitepapers/esgsolutionshowcasesplunkmay2015.Pdf

Pagliery, J. (2014). Half of American adults hacked this year. Retrieved from http://money.cnn.com/2014/05/28/technology/security/hackdatabreach/

Pellicane, C. & Blaho, J.A. (2015). Lessons learned from adapting the NSF I-Corps curriculum to undergraduate engineering student entrepreneurship training. Retrieved from http://venturewell.org/open/wp-content/uploads/2013/10/PELLICANE.pdf

Seoul Framework. (2013). Seoul framework for and commitment to open and secure cyberspace. Seoul Framework on Cyberspace. Retrieved from http://www.mofat.go.kr/english/visa/images/res/SeoulFramework.pdf

STOP.THINK.CONNECT. (2016). About STOP.THINK.CONNECT. U.S. Department of Homeland Security. Developed by The AntiPhishing Working Group (APWG) and National Cyber Security Alliance (NCSA). Retrieved from https://stopthinkconnect.org/about

Topper, A. M. & Powers, J. M. (2013). Democracy's college: The American community college in the 21st Century: Framing the issue. *Education Policy Analysis Archives*, 21 (14).

U.S. Census Bureau. (2014). Census on educational attainment. Retrieved from http://www.census.gov/hhes/socdemo/education/data/cps/2014/tables.html

Weise, E. (2014). 43% of companies had a data breach in the past year. *USA TODAY*. Retrieved from http://www.usatoday.com/story/tech/2014/09/24/databreachcompanies60/16106197/

WeLiveSecurity. (2012). Retrieved from http://www.welivesecurity.com/2012/10/10/studyfinds90percenthavenorecentcybersecuritytraining/

White House Fast Facts. (2013). Retrieved from https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

White, G. L., Hewitt, B., & Kruck, S. E. (2013). Incorporating global information security and assurance in I.S. education. *Journal of Information Systems Education*, 24 (1), 1116.

Woerner, R. (2012). Security education vs. training: Understand the difference and plan appropriately to meet your goals. *Information Security*. May: 67.

Young, J. (1997). Community economic development through community colleges. *New Directions for Higher Education* 1997 (97): 7483.

AUTHORS

Benito R. Fernández, PhD, (benito@utexas.edu) is an associate professor of mechanical, biomedical, and manufacturing systems engineering in The University of Texas at Austin. He received his chemical engineer and materials engineer degrees in 1979 and 1981 respectively from Universidad Simón Bolívar, Sartenejas, Venezuela; and his Master of Science (1986) and doctoral (1988) degrees from the Massachusetts Institute of Technology. Fernández had faculty appointments at USB (1979–1981), Texas A&M (1988–1990), and UT Austin since 1990. He is the director of the NERDLab (NeuroEngineering, Research & Development Laboratory), where he has been working on research and development of "applied intelligence systems" (Artificial Neural Networks, Fuzzy Systems, Genetic Algorithms, Artificial Immune Systems, Evolving Systems, etc.). He also founded and directs the Advanced Mechatronics laboratory in UT. Research and teaching interests include mechatronics, eXtreme devices, Resilient & Secure CyberPhysical Systems, applied intelligence, OptimallyRobust Diagnostics & Control, evolutionary systems, design and manufacturing. Fernández has published over 90 referenced articles, has organized and co-chaired several international conferences, has five patents (four issued, one pending), and was associate editor of the International Journal of Smart Engineering System Design. He is a member of IEEE, ASME, and INNS.

Carlos A. García, BS, CS, (garcia.carlos@utexas.edu) is a visiting scholar at The University of Texas at Austin. García has a Bachelor of Science in computer science engineering from Universidad Simón Bolívar (1998). He has advanced expertise in storage technologies, Unix-based operating systems and networking solutions. García has more than 17 years of experience working for multi-national companies as a senior sales engineer and business developer. García worked with complex technologies and IT solutions in Cisco, EMC, and Hitachi Data Systems, for large industrial accounts. He has one patent pending.

José R. Capriles, BS, EE, MS, (capriles@utexas.edu) is a doctoral candidate in the Mechanical Engineering Department at The University of Texas at Austin. He has a Master of Science in automated control and robotics (2012) from I RI (Institut de Robòtica i Informàtica Industrial), CSICUPC (Universitat Politècnica de Catalunya); and Bachelor of Science in electronic engineering from Universidad Simón Bolívar (2009). His expertise includes electronic circuits design and programming. Capriles' doctoral research is in the hybrid computer development. Before starting his doctoral studies, Capriles worked for two years as a robotics engineer in PAL Robotics (Barcelona). He has one patent pending.

Wendy Ford, PhD, (wford@qcc.cuny.edu) is an associate professor of computer information systems at Queensborough Community College in the Business Department. She is the co-chair of the Curriculum Committee for the Business Technology Early College High School Program and a participant in the National Initiative for Cybersecurity Education K–12 Subgroup. Prior to joining the faculty at QCC, she was an information systems consulting manager for Ernst & Young and she also designed and managed information systems for McGraw-Hill. Her research interests include information assurance and business information systems.

Christine Mooney, Esq., (cmooney@qcc.cuny.edu) is a an associate professor at CUNY's Queensborough Community College. Professor Mooney is an attorney licensed to practice law in the state of New York. Prior to her appointment as a faculty member, she served as the director of human resources at LaGuardia Community College. In that capacity, she was responsible for the design and implementation of staff training programs. She received her Juris Doctor from New York Law School with honors. She serves as a member of the University Committee on Student Entrepreneurship. She concurrently serves as the co-program director of the Community College Innovation Challenge and is a faculty mentor for student cohorts in the New York State Business Plan Competition. In 2015, her team was invited to compete in the finals of the New York State Business Plan competition. She and the members of her team received the Esprit de Corps award in the Energy/Sustainability category. Her team was the only community college to receive the award statewide.

Meeting the Present and Future Demands of Cybersecurity

Kevin K. Lemmon

ASSESSING THE DEMAND FOR CYBERSECURITY PROFESSIONALS

Executive Order 13587, issued by President Obama, mandates that every U.S. government agency that has classified information—in effect, all of them—must have an insider threat program in place. This mandate was followed by the Cybersecurity Strategy and Implementation Plan (CSIP) in late 2015. After that, the National Industrial Security Operating Manual (NISPOM) Conforming Change 2, released in May 2016, made similar mandates for all contractors that work with government classified information. Typically, IT departments have focused on cyber threats—also known as outside threats—for a long time now. Typical cyber threats include malware, distributed denial of service (DDOS) attacks, viruses, rogue nation attacks, fraud, theft, and ransomware. Ransomware attacks, which are occurring more frequently, are fairly easy, low-risk/high-reward attacks for the common hacker. Essentially, the hacker is telling the victim to, "pay up, or you will never get your data back," as they demand $500 for an individual or $10,000 (on average) for a mid-size company. Insider threats have always existed but do not demand the same "front page news" media coverage as cyber-attacks receive. Edward Snowden changed all this in 2013 by releasing millions of classified documents while employed as a National Security Agency (NSA) contractor. So to have an effective security defense, companies and organizations must protect their perimeters and data from inside threats.

A cybersecurity program is the number one priority for U.S. government agencies and is usually found in the top three initiatives by CEOs of any U.S. corporation. Lloyd's of London, the British insurance company, states cyber-attacks cost companies over $400 billion every year (Gandel, 2015). A survey by SpectorSoft in mid-2015 says that 62% of corporations showed in increase in insider attacks, and that the average remediation cost is $445,000 per breach (InformationWeek, 2015). The cost to an average U.S. corporation can be measured in millions of dollars of lost revenue per hour, and the lost confidence of clients can last for years. For government agencies, the loss can be measured in human lives as hackers gain access to our critical power grid, blueprints of military equipment, or—as in the recent Office of Personnel Management (OPM) breach—the personal information of millions of U.S. citizens with government clearances.

DOES THIS CLOUD HAVE A SILVER LINING?

Yes, it does. The recruitment and retention of a highly-qualified cybersecurity workforce is one of the top five initiatives issued from the Executive Office of the President. It is also typically found within the top three cybersecurity concerns when CEOs are interviewed. Talent cannot be trained or recruited fast enough to keep up with the demands in this critical space. *Forbes* magazine estimates that there will be one million cybersecurity job openings in 2016. Demand is expected to rise to 6 million globally by 2020, as predicted by Michael Brown, CEO at Symantec. An average salary in the software security field is $85,000 and a chief security officer can expect to earn approximately $225,000 in this field (Morgan, 2015).

Where a four-year degree was required a few years ago, now these jobs are available to young people just starting their careers or seasoned workers looking to make a career change. There are numerous cybersecurity classes offered online and at local community colleges. Recently, community colleges began working closely with government agencies such as the NSA and the Department of Homeland Security (DHS) to develop cybersecurity programs. This solution allows an alternative to a four-year degree program, providing a quicker solution to government and commercial sector demands. Because of the accessibility, lower tuition rates, and, in most cases, an open-door admission policy, this option is attractive for minorities, women, and lower-income students. This is what government and corporations alike are demanding—a quickly, well-trained workforce to take on the cyber threats of today and tomorrow.

There are several organizations that help support these groups in the workplace. For example, Women in Technology, or WIT (WomeninTechnology.org), offers career sessions, mentoring, and even a special focus on cybersecurity and information technology (IT) jobs. There are scores of other organizations which were established to assist women and minorities enter this crucial job market. Many can be found at the National Initiative for Cybersecurity Careers and Studies (niccs.us-cert.gov). The International Consortium of Minority Cybersecurity Professionals (icmcp.org) serves the international minority community with courses, mentoring, and job seeking events. There has never been a better time to join an industry that is not only critical to government agencies and corporations alike, but will give citizens a chance to make a measureable difference in the protection of data and people.

There has to be a quicker, easier approach to the cybersecurity staffing concerns for the present as well as the future. The demand is real and the stakes are high. Hackers are well-trained, sponsored, and more sophisticated in their attacks. Cybersecurity is not just about protecting a company's important data, but protecting our nation's critical infrastructure including vulnerable power grids. The breaches coming from malicious hackers, accidental insiders, and rogue nations continue to increase in volume and sophistication. They are being conducted for profit, for hacktivism, and for cyber warfare. Our first line of defense must be a well-trained and rapidly-deployed workforce to counter the global threat.

REFERENCES CITED

Gandel, S. (2015). Lloyd's CEO: Cyber attacks cost companies $400 billion every year. *Fortune Magazine*. Retrieved from http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/

InformationWeek DarkReading. (2015). Survey shows Insider threats on the rise; organizations experience an average of 3.8 attacks per year. Retrieved from http://www.darkreading.com/vulnerabilities--threats/survey-shows-insider-threats-on-the-rise-organizations-experience-an-average-of-38-attacks-per-year/d/d-id/1321069

Morgan, S. (2015). Cybersecurity job market to suffer severe workforce shortage. *CSO Online*. Retrieved from http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html

AUTHOR

Kevin K. Lemmon is a seasoned software security leader specializing in building and managing sales engineers. He is the senior director of solution engineers at Distil Networks, a global leader in bot detection and mitigation. Lemmon has also led teams at Symantec, ArcSight, HP, and Securonix. He resides in the Washington, DC metro area.

2 Plus 2 Cybersecurity Education—Transfer Pathways for Women and Minorities

Laila Khreisat, PhD | Neelu Sinha, PhD

ABSTRACT

Since 2001, Fairleigh Dickinson University's (FDU's) Community College Partnership Program has brought bachelor's and master's degrees to underrepresented areas of New Jersey, making 2 plus 2 transition seamless, as advisers from both institutions help students (who receive generous academic scholarships) stay on track for associate and bachelor's degree. Our goal is to expand this and bring *cybersecurity education* within reach of *women* and *minorities* who are vastly underrepresented in our nation's cybersecurity workforce. More than half of first generation college students from lowest income quartiles (majority being women and minorities) use community college as an entry point to a four-year degree; however, only a small percentage actually transition and graduate. Apart from their inherent, complex life circumstances and personal barriers, *institutional factors* hinder their transition—including informational setbacks related to advising, conventional pedagogy, real-world disconnects, and resource limitations. We explore innovative ways to mitigate these hindrances and provide a radical pedagogical overhaul to retain their interests in cybersecurity.

A tier-based mentoring initiative aims to increase transfer students' confidence and persistence. Dedicated faculty advisors (Tier I) work closely with a liaison to follow a formal credit transfer process; peer mentors (cybersecurity majors) (Tier II) provide mentoring and support inside and outside the classroom. We build on FDU's success with the Support Our Students (SOS) program (structured academic support system to foster increased sense of confidence) to provide learning experiences for transfer students that focus on culturally sensitive teaching and application based, hands-on experiences in cybersecurity.

INTRODUCTION

Increasing frequency of cyber-attacks has created a major demand for qualified cybersecurity professionals. Government, non-profit organizations, and businesses all over the world are seeking professionals to reinforce their defenses against such attacks. However, there are not enough qualified and skilled professionals available. Workforce shortages in the cybersecurity field are challenging and have been widely documented. Community colleges (CCs) help thwart some of these challenges and are well-known for providing low-cost education with smaller class sizes and faculty focused on teaching. They enable students to continue to live at home—further reducing costs—and also offer excellent student support services with a variety of programs of study. While CCs help mitigate some of the workforce shortages, they only prepare students for entry-level positions. Many of the cybersecurity-related occupations, as described by the Bureau of Labor Statistics, require a four-year college degree at the minimum. Thus, a pipelined approach is needed whereby CCs and four-year degree colleges form a partnership to make bachelor's and master's degrees accessible to these students. Several universities and CCs already have such partnerships in place—for example Fairleigh Dickinson University's Community College Partnership program helps students stay on track for associate and bachelor's degrees. Apart from the workforce shortages, another major concern is the lack of diversity. Women and minorities are vastly underrepresented in our nation's cybersecurity workforce. Our goal is to expand FDU's pipelined approach and bring cybersecurity education within reach of women and minorities. More than half of first generation college students from the lowest income quartiles (the majority being women and minorities) use community college as an entry point to a four-year degree; but only a small percentage actually transition and graduate. Apart from their inherent, complex life circumstances and personal barriers, institutional factors such as informational setbacks related to advising, conventional pedagogy, real-world disconnects, and resource limitations, hinder their transition. We explore innovative ways to mitigate these hindrances and provide a radical pedagogical overhaul to retain their interests in cybersecurity and build a diverse cybersecurity workforce that can help businesses and government bulk up their defenses.

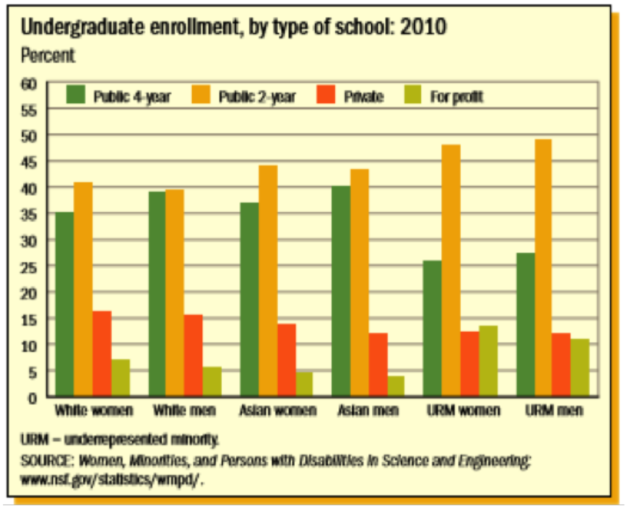
Our goal is to expand existing programs at FDU including the Community College Partnership (CCP) and Support Our Students (SOS) to prepare women and minorities for cybersecurity education. We propose an innovative two-tier mentoring program, which along with a radical pedagogical approach (based on real-world problem solving using modern equipment) supplemented with hands-on research (with faculty) can provide learning experiences for transfer (women and minority) students that focuses on culturally sensitive teaching, and application-based, hands-on experiences in cybersecurity. We hope to increase the confidence and nurture the persistence of our women and minority transfer students as they embark on their journey from CCs to FDU and beyond.

LITERATURE REVIEW

In March 2015, Peninsula Press (Setalvad, 2015) reported that more than 209,000 cybersecurity jobs in the U.S. were unfilled (based on analysis of numbers from the Bureau of Labor Statistics), with a 74% increase in job postings over the last five years alone. Earlier this year, *Forbes* (Morgan, 2016), citing a report (Cisco, 2014), proclaimed one million cybersecurity job openings worldwide in 2016, with the market expected to grow to $170 billion by 2020, up from $75 billion in 2015. To protect against industrialized adversaries, Cisco's 2016 Annual Security Report sounds a global "call-to-arms" for greater collaboration and investment, not only in the processes and technologies, but also in people (Cisco, 2016). In 2015, Cisco highlighted a cybersecurity talent gap, and cautioned that while demand for cybersecurity skills was high, the supply fell short. The Bureau of Labor Statistics (BLS) (2015) lists the typical entry-level education requirement for many of these cybersecurity related occupations as a bachelor's degree.

In addition to the talent gap and workforce shortages, lack of diversity in cybersecurity is a significant problem. In their 2013 report, the National Science Foundation's National Center for Science and Engineering Statistics provided statistical information about the participation of women, minorities, and persons with disabilities in science and engineering education (Figure 1), which clearly shows that underrepresented minorities—Blacks, Hispanics, and American Indians—enroll in disproportionately higher numbers in public two-year colleges and, along with women, in for-profit academic institutions.

FIGURE 1: Undergraduate Enrollment By Type of School



URM – underrepresented minority.

SOURCE: *Women, Minorities, and Persons with Disabilities in Science and Engineering*; www.nsf.gov/statistics/wmpd/.

With the BLS projecting a shortfall of qualified individuals to fill cybersecurity related positions and the fact that approximately half of our nation's college students (a majority of which are women and minorities) begin their studies at community college, there is an urgent need to overhaul the transfer process and increase the efficacy of the community college transfer pathways at the national level. We need a deeper understanding about the issues affecting the transfer pathways—particularly for women and minorities—in order to improve retention and bring diversity in cybersecurity fields. The high costs of unnecessary delays while navigating CC transfer pathways are undeniable (Packard, Gagnon, and Senas, 2012), particularly in science, technology, engineering, and mathematics (the so-called STEM) fields. A student's transfer progress takes place within a larger social ecology (Bronfenbrenner, 1979) and is influenced by many factors including intraindividual (student success strategies and personal resources) and institutional factors including the effectiveness of a college's transfer function (Hagedorn, Cypers, and Lester, 2008).

The success of any program designed to attract and retain underrepresented students in STEM and cybersecurity depends not only on the typical approaches of providing academic services and resources including research opportunities and advising to name a few, but also on the following three factors (Dyer-Barr, (2013)): 1) the program should provide a student-centered approach that develops academic and personal relationships with the students, 2) the program should provide means for community building, where students develop a sense of belonging with other minority students, 3) and collaboration at different levels to ensure that students receive services and information in the most efficient and timely manner.

Maton & Hrabowski, (2004) and Maton, Hrabowski, and Schmitt (2000) present other factors essential to increasing the participation of minority in STEM similar to the previous three, which include 1) academic and social integration, 2) knowledge and skill development, 3) support and motivation, and 4) monitoring and advising. Lou, Shih, Diez, and Tseng (2010) explored the effects of problem-based learning (PBL) strategies on the attitudes of female senior high school students toward integrated knowledge learning in STEM. The results of their study indicate that PBL strategies not only enhance students' attitudes toward STEM learning and the exploration of future career choices but also provide them with experiences related to knowledge integration and application. They further recommend that the curriculum should include more content related to specialty subjects to enhance their technological capabilities and a learning mechanism should be offered to aid advisers or teachers in strengthening students' integrated and systematic knowledge about STEM.

Another approach adopted by many computer science educators is to use Active Learning (AL) techniques and we have previously shown how technology can be used in creative ways to promote AL to help meet some of the challenges of teaching many different CS courses (Sinha, 2007; Sinha, Khreisat, and Sharma, 2009). A related approach is to use AL in collaborative programming and problem solving environments as in the Treisman model, which was originally designed for the first-year calculus course and involved intensive workshops where students collaborated in small groups to solve problems. Chinn, Martin, and Spencer (2007) adapted this model for two CS courses and concluded that the workshop model can be an effective learning environment for students in courses primarily involving analysis, but for courses that involve large amounts of programming, further adaptations to the model might be needed. Several studies (Tinto, 2012, President's Council of Advisors on Science and Technology, 2012; Fullilove & Treisman, 1986; Horwitz, 2009; Kosciuk, 1997; Millar, Alexander, Lewis, and Levin, 1995) have shown that peer-led learning is a successful approach that utilizes active learning and collaboration to motivate and engage students leading to improved academic performance. In fact shows that peer-led team learning increases "participation and success of under-represented groups in Introductory Computer Science" (Horwitz 2009).

COMMUNITY COLLEGE PARTNERSHIP PROGRAM AT FDU

Fairleigh Dickinson University has a well-established Community College Partnership program with several community colleges in New Jersey, which includes Atlantic Cape Community College, Rowan College at Gloucester County, Rowan College at Burlington County, Camden County College, Mercer County College, Ocean County College, Cumberland County College, and County College of Morris (in the process of being finalized at the time of this writing). The partnership program is designed to help students stay on track for associate and bachelor's degrees. The program is convenient and flexible in that it provides on campus classes, evening and Saturday classes as well as accelerated options for some degrees where a semester consists of two seven and a half weeks terms allowing a student to complete up to 18 credits per year. Students have the option to enroll as full-time or part-time students. This approach offers a great deal of promise to provide transfer students with opportunities to pursue their degrees in the field of cybersecurity. Each community college has a liaison who works closely with academic departments and advisors at FDU to streamline the transfer process for each student.

SUPPORT OUR STUDENTS (SOS) PROGRAM

The SOS program at FDU's Metropolitan campus was started in 1990 to provide structure and support to students. It is not a program for developmental (remedial) students. The structural components of the program aim at reinforcing classroom material and monitoring the academic performance of students. This is achieved using assessment techniques such as frequent quizzes to gauge students' understanding, several graded homework assignments that are returned promptly to provide students with feedback, and group study sessions once a week providing students with the opportunity to work in groups to solve problem sets which are graded and returned to students. Four hourly exams are held for each course—these take place early in the morning outside of the class time, providing students with the opportunity to start the exam early and allowing extra time to complete the exam. Instructors post all class materials online and they follow a standard grading policy. The program provides support to students by holding early morning exams with additional time which is preceded by free breakfast; each student receives detailed assessment reports that include grade averages and suggestions for improving performance. Students are praised for doing well and receive recognition for their achievement. Students who receive grades of "B" or better are given a gift, and students who receive an "A" average after completing three quarters of the semester will be treated to a trip. The SOS program has been very successful and has resulted in a dramatic decrease in student failure rates while maintaining academic standards.

For our mentoring program we will adapt the idea of group work to include peer-led groups in classes as well as peer-led groups outside the classroom.

2 PLUS 2 CYBERSECURITY EDUCATION

TWO-TIER MENTORING

We propose a two-tier mentoring program for transfer students that starts during their time at the community college. Currently each community college has a liaison who works closely with academic departments and advisors at FDU to streamline the transfer process for each student (Tier I). Through the Community College Partnership program, formal articulation agreements are in place that clearly define the courses transferrable from the community college to FDU, providing students with a guide to plan for the two years at the community college as well as the upcoming two years at FDU with the help of their academic advisor at the community college and a liaison. After successfully transferring to FDU, students will be assigned dedicated faculty advisors to guide and advise them throughout their 2 years at FDU. This level of advising ensures that students stay on track with their course work towards graduation.

The second level of mentoring (Tier II) consists of student mentors and leaders (peer mentors) who are computer science majors. Peer mentors provide mentoring and support inside and outside the classroom. In this level we will implement the *peer-led group learning approach* where students are organized into small groups inside the classroom to work on projects and assignments, providing them with the experience of working on collaborative problem solving.

Each group is assigned a group leader (peer mentor), an upper-level computer science major who will provide guidance and support. The leader will track the group's performance to ensure completion of the tasks at hand and provide guidance and support as appropriate. The leaders are not tutors and will not provide solutions to assignments and projects.

This approach will be implemented in an introductory computer science course—namely, CSCI 2216 Introduction to Computer Science II—which transfer students will take when starting at FDU. Our curriculum in computer science contains a sequence of three programming courses that provide students with the necessary skills to succeed in subsequent courses in computer science. The first course, CSCI 1205 Introduction to Computer Programming, introduces students to programming in Visual C#, and the second course, CSCI 2215 Introduction to Computer Science, introduces students to programming in C++. Incoming transfer students usually have taken programming courses that transfer in as CSCI 1205 and CSCI 2215. So they will take our third programming course, CSCI 2216 Introduction to Computer Programming II, which was recently introduced to provide students with more advanced programming skills in C++. Since this will be one of the first courses that transfer students take at FDU, we will utilize the peer-led group learning approach.

We will also develop a mentorship program outside the classroom for our cybersecurity courses. For every cybersecurity course there will be a peer-led group that meets once a week for two hours outside the classroom providing students the opportunity to work on problem-solving and projects in a group environment under the guidance and support of the group leaders. Students must attend the group sessions at no extra cost to them and they will receive a pass/fail grade.

The Computer Science Society and The Women in Computer Science (WICS) Society are active within our department and hold a wide range of events every semester. The WICS society recently received a grant from The National Center for Women & Information Technology (NCWIT) and Google as seed money to start the society. The funds are being used to hold Hours of Code and off-campus trips. Invitations go out to all students for events, so this provides opportunities for transfer students to engage in extracurricular activities and help them become acquainted with fellow computer science majors.

RECRUITMENT PROCESS

Computer science majors will be recruited to become peer leaders, starting in their sophomore year. We will identify underrepresented students for peer leadership positions to provide them with leadership opportunities, which—as studies show—increase their confidence levels and provide them with a sense of belonging. These opportunities help to increase student retention and academic success. After their first semester at FDU, transfer students will have the opportunity to apply for peer leader positions. For outside-the-classroom mentorship, cybersecurity students will be recruited as peer leaders. As part of the recruiting process, a workshop will be held at the beginning of every semester to provide training on leadership skills and mentoring as well as culturally sensitive pedagogy. Weekly meetings with faculty will also be held to track student progress and identify any issues and problems that the leaders are facing.

CULTURAL RESPONSIVE TEACHING

Culturally responsive teaching is a student-centered pedagogical approach that focuses on the student's cultural strengths in designing course content and delivery methods to ensure student achievement and success (Ladson-Billings, 1994). Diaz-Rico & Weed (2010) state that learning is affected by cultural elements including family structure, beliefs, and values as well as communication and roles of individuals in society. Motivating students to learn leads to their engagement in the learning process. According to Wlodkowski & Ginsberg (1995), there are four motivational conditions that should be part of a culturally responsive teaching model:

1. Establishing inclusion: setting up a learning environment where students and teachers have mutual respect and feel connected to one another.
2. Developing attitude: by making the course content relatable to students we create a favorable disposition toward the learning experience.
3. Enhancing meaning: develop learning experiences that take into account students' perspectives and values will make the experiences more meaningful, thoughtful, and challenging.
4. Engendering competence: students learn and understand (more effectively) concepts that they value.

Ladson-Billings, (1994) listed the characteristics of culturally responsive teaching as the following:

1. Communication of High Expectations
2. Active Teaching Methods
3. Practitioner as Facilitator
4. Inclusion of Culturally and Linguistically Diverse Students
5. Cultural Sensitivity
6. Reshaping the Curriculum or Delivery of Services
7. Student-Controlled Discourse
8. Small Group Instruction

Cultural responsive teaching in our project will be implemented through the use of Active Learning in the classroom where students actively participate in learning. Additionally, students are provided with research opportunities (characteristic 2); the use of peer-led groups inside the classroom and mentoring outside the classroom (characteristics 3, 7, 8); the opportunities to develop assignments and activities as well as in class examples that contain culturally relevant materials relatable to the students (5, 6); and faculty development seminars on cultural pedagogy and equity in education through our partnership with the National Alliance for Partnerships in Equity Education Foundation (NAPE) to train faculty on culturally responsive teaching (3, 5). Our student population is diverse and we expect it to stay so and possibly become more diverse in the future, especially as we witness an increase in the number of female students majoring in computer science (characteristic 4).

PEDAGOGICAL APPROACH

In addition to the two-tier mentoring approach, we will use the Active Learning approach (Sinha, Khreisat, and Sharma, 2009) to engage students in our classes, which is particularly effective in cybersecurity education where we deal with real-time attacks and issues. In this instruction method, students actively participate in their learning process via learner-centered activities that exercise their higher-order thinking skills of analysis, synthesis, and evaluation rather than passively listening to a lecture. Interaction (between students and content, between students and instructors, between students and their tools, and among students) is a key element in active learning and in the implementation of Chickering and Gamson's (1987) seven principles (Chickering and Ehrmann 1996). Incorporating interaction between students and technology using mobile devices and pen-based tablet computers has shown to enhance learner-interface interaction in our classes. In addition, based on the ten core principles for designing effective learning environments (Boettcher, 2007), we use an innovative methodology based on Active Student Centered Learning, or ACSL (Sinha, 2007). Figure 2 shows the ASCL as a relational model with the student or learner in the center, supported by faculty as well as the environment, resources, and tools.

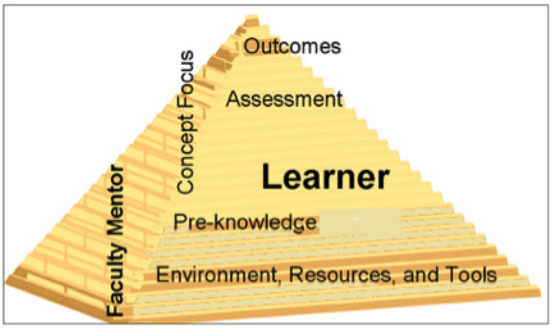


FIGURE 2: ASCL RELATIONAL MODEL

We are currently attempting to implement another pedagogical approach—Media Computation at Georgia Tech (Case Study 1)—in our introductory CS classes, which has been shown to be successful at several institutions. In this approach, we emphasize creative learning environments to make course content relevant even to non-CS students and at the same time foster a positive social climate in the class. For this we use modern hands-on prototyping platforms such as the Arduino microcontroller and Raspberry Pi microprocessors, which are very affordable, and allow the students to unleash their creativity without fear of breaking something expensive. These platforms are relatively new and are becoming popular, particularly due to the advent of the Internet of Things (IoT) whereby machines talk to other machines without human intervention via sensors which can be easily controlled by mobile devices. Our introductory programming courses are perfect for teaching students how to create applications for controlling such sensors via their smart phones and tablets over the Internet with simple projects such as controlling a thermostat or turning on lights remotely. We hope that this "tinkering" approach (on relatively cheap devices) will spark curiosity in students—particularly women and minorities—as they help link real-world problems and solutions into our courses. We also hope to reach out to students who are non-STEM majors since they hear about modern technology in the media and would love to explore these in the classroom.

RESEARCH WITH FACULTY

Another way to improve educational experiences of transfer students (especially women and minorities) from CCs is to involve them in research with a faculty member. This kind of enriching experience is often lacking in CCs and research has shown (Evans, Heyl, and Liggit, 2016) that exposing students to research with faculty members helps them succeed as scientists in academia and further fosters development and improvement of their potential and competency as the next generation of investigators. The cybersecurity field is ripe for research and many FDU faculty members are pursuing research in various cybersecurity and information assurance topics. The National Security Agency (NSA) and the Department of Homeland Security (DHS) have designated FDU as a National Center of Academic Excellence in Information Assurance Education and Cyber Defense (CAE/IAE/CD) through 2020. FDU's Center for Cybersecurity and Information Assurance fosters awareness, promotes research activities of students, and cultivates the next generation through community outreach programs, making FDU a viable route for CC transfer students. In order to generate an educated cybersecurity workforce, research training and opportunities (offered to all especially women and minorities) need to be at the forefront of all college programs.

PROJECT ASSESSMENT

Several assessment instruments will be employed to study the impact of our project on student retention, success and graduation rates. Surveys will be used to assess students' attitudes and perceptions. Both pre- and post-project surveys will be developed. Focus groups will be held with students to further collect information during each semester. All incoming transfer students will be tracked throughout their time at FDU to evaluate their progress towards graduation.

CONCLUSIONS

Building on our well-established Community College Partnership program and our SOS programs targeted to women and minorities, we hope to build a pipeline of diverse cybersecurity workforce, by providing transfer students with opportunities to pursue their degrees in this field. Offering a two-tier mentoring program from the time transfer students begin at FDU will help ensure that they stay on track with their course work towards graduation. In addition, culturally sensitive teaching along with modern pedagogical approaches will help us retain these students. Research with faculty will help these students gain confidence and increase their potential to cultivate them into the next generation of cybersecurity workforce professionals.

REFERENCES CITED

Boettcher, J. (2007). Ten core principles for designing effective learning environments: Insights from brain research and pedagogical theory. *Innovate – Journal of Online Education*, Vol. 3, Issue 3.

Bronfenbrenner, U. (1979). *The ecology of human development*. Cambridge, MA: Harvard University Press.

Bureau of Labor Statistics Occupational Outlook Handbook. (2015).Retrieved, from http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

Chickering, A. & S. Ehrmann. (1996.) Implementing the seven principles: Technology as lever. *American Association of Higher Education Bulletin*, (October): 3–6.

Chickering, A. &Z. Gamson. (1987.) Seven principles of good practice in undergraduate education. American *Association of Higher Education Bulletin*, (March): 3–7.

Chinn, D., Martin, K., & Spencer, C. (2007). Treisman workshops and student performance in CS. Proceedings of the 38th SIGCSE *Technical Symposium on Computer Science Education* - SIGCSE '07. doi:10.1145/1227310.1227383.

Cisco. (2014). Security Capabilities Benchmark Study. Retrieved from http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2015_ASR.pdf.

Cisco. (2016). Annual Security Report. Retrieved from http://www.cisco.com/c/dam/assets/offers/pdfs/cisco-asr-2016.pdf

Diaz-Rico L. T. & Weed K. Z. (2010), *The Crosscultural, language, and academic development handbook: A complete K-12 reference guide* (4th ed.). Boston, MA: Pearson.

Dyer-Barr, R. (2013). What works in STEM intervention programs (SIPs) for undergraduates: Perspectives from SIP Administrators. 2013 *ASQ Advancing the STEM Agenda Conference*, June 3–4, 2013.

Evans, H. G., Heyl, D. L., and Liggit, P. (2016). Team-based learning, faculty research, and grant writing bring significant learning experiences to an undergraduate biochemistry laboratory course. *J. Chem. Educ. Journal of Chemical Education*. doi:10.1021/acs.jchemed.5b00854

Fullilove, R. & Treisman, P. (1986). Mathematics achievement among African-American undergraduates in the University of California, Berkeley: An evaluation of the mathematics workshop program. *The Journal of Negro Education*, 59(3):463–478, 1986.

Hagedorn, L. S., Cypers, S., and Lester, J. (2008). Looking in the review mirror: Factors affecting transfer for urban community college students. *Community College Journal of Research & Practice*, 32(9), 643–664.

Horwitz, S. (2009). Using peer-led team learning to increase participation and success of under-represented groups in introductory computer science. Univ. of Wisconsin–Madison Madison WI, USA, SIGCSE 2009.

Kosciuk, S. (1997). Impact of the Wisconsin emerging scholars first-semester calculus program. Technical report, LEAD Center, University of Wisconsin-Madison, July 1997.

Ladson-Billings, G. (1994). *The dreamkeepers*. San Francisco: Jossey-Bass Publishing Co.

Ladson-Billings G. (1995), Toward a theory of culturally relevant pedagogy. *American Education Research Journal*, Vol. 32, No. 3, pp. 465–491.

Lou, S., Shih, R., Diez, C. R., and Tseng, K. (2010). The impact of problem-based learning strategies on STEM knowledge integration and attitudes: An exploratory study among female Taiwanese senior high school students. *International Journal of Technology and Design*, 21(2), 195–215. doi:10.1007/s10798-010-9114-8.

Maton, K., & Hrabowski, F. (2004). Increasing the number of African American PhDs in the sciences and engineering: A strengths-based approach. *American Psychologist*, 59, 547–556.

Maton, K., Hrabowski, F., and Schmitt, C. (2000). African American college students excelling in the sciences: College and post-college outcomes of the Meyerhoff Scholars Program. *Journal of Research in Science Teaching*, 37(7), 629-654.

Media Computation at Georgia Tech (Case Study 1). (n.d.). Retrieved June 10, 2016, from https://www.ncwit.org/resources/how-does-engaging-curriculum-attract-students-computing/media-computation-georgia-tech

Millar, S., Alexander, B., Lewis, H. and Levin, J. (1995). Pilot Wisconsin emerging scholars program, 1993–94, Technical report, LEAD Center, University of Wisconsin-Madison, March 1995.

Morgan, S. (2016). One million cybersecurity job openings in 2016. Retrieved May 22, 2016, from http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#1dd7de927d27

National Science Foundation, National Center for Science and Engineering Statistics. (2013). Women, minorities, and persons with disabilities in science and engineering: 2013. Special Report NSF 13-304. Arlington, VA. Available at http://www.nsf.gov/statistics/wmpd/.

Packard, B. W., Gagnon, J. L., and Senas, A. J. (2012). Navigating community college transfer in science, technical, engineering, and mathematics fields. Community *College Journal of Research and Practice*, 36(9), 670–683. doi:10.1080/10668926.2010.495570.

President's Council of Advisors on Science and Technology. (2012). Engage to excel: Producing one million additional college graduates with degrees in Science, Technology, Engineering, and Mathematics.

Setalvad, A. (2015). Demand to fill cybersecurity jobs booming. *Peninsula Press, A Project of Stanford_Journalism*. Retrieved May 22, 2016, from http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/

Sinha, N. (2007). An active student centered learning (ASCL) approach to instruct and assess a software engineering course. *International Journal of Instructional Technology and Distance Learning*, Volume 4, Number 6, ISSN 1550-6908, Jun 2007.

Sinha, N., Khreisat, L. and Sharma, K. (2009). Learner-interface interaction for technology-enhanced active learning. Innovate *Journal of Online Education*, 5(3). February/March 2009.

Tinto, V. (2012). *Completing college* - rethinking institutional action. The University of Chicago Press.

Wlodkowski, R.J. & Ginsberg, M.B. (1995). A framework for culturally responsive teaching. September 1995, Volume 53, Number 1. *Strengthening Student Engagement*, 17–21.

AUTHORS

Laila Khreisat, PhD, (khreisat@fdu.edu) is an associate professor in computer science at Fairleigh Dickinson University (FDU). She received her Master of Science in computer science from Columbia University in 1994, and her doctoral degree from The City University of New York (CUNY) in 2000. She was a Fulbright scholar from 1992 to 1994 and is the co-principal investigator for the HP technology grant awarded in 2007, as well as co-principal investigator on the Teaching to Increase Diversity and Equity in STEM grant from the Association of American Colleges & Universities (AAC&U) awarded in 2014. She is the chair of the Math, Computer Science and Physics Department at FDU. Her current research interests include data mining and the impact of new technology and tools on teaching and pedagogy.

Neelu Sinha, PhD, (Sinha@fdu.edu) is an associate professor in computer science at Fairleigh Dickinson University (FDU). She earned her Master of Science and doctoral degree in electrical and computer engineering from Iowa State University, Ames, Iowa. She has over 11 years of industrial experience from Control Data Corporation, Empros International, Bellcore, and Bell Laboratories (AT&T, Lucent, Alcatel-Lucent). She has also taught at the University of Minnesota and New Jersey Institute of Technology. Her current areas of research are in developing security applications for cloud computing and mobile platforms.

Community Colleges’ Outreach Role in Cybersecurity

Debra A. Nakama, PhD

ABSTRACT

With a high proportion of diverse and non-traditional students enrolled in rural community colleges, these institutions have a critical outreach role in expanding access to cybersecurity careers. Moreover, focusing on women and minorities early presents an important opportunity to improve the economic security for a wider and diverse range of students they serve. This community college case study focuses on an early-admit outreach high school approach conducted in fall 2015 of 41 high school women and minorities to promote a cybersecurity career pathway trajectory in rural communities who may not have access to cybersecurity courses while in high school. The primary purpose of this paper is to offer administrative insights for the need to offer outreach cybersecurity education at rural high schools. Another purpose of this paper is to shed light on the need for outreach recruiter agents and their role in increasing the number of women and minorities in the cybersecurity workforce pipeline. The study’s initial reflective action highlights how to: (1) cross educational sector boundaries to transition from internal optimization to external interaction; (2) orchestrate resources to create a learning collective; and (3) use an iterative process to discover integrative ways to engage a broader, more diverse group of students in cybersecurity.

INTRODUCTION

The community college connection to high schools is broad in scope and continues to increase via a number of models that offer early college admit options (Morest & Karp, 2006; Bragg, 2013). In addition, community colleges are central in focusing on this new wave of America’s high school women and minorities in initiatives to improve their labor market prospects (Osterman, 2012). This paper describes a post-secondary collaboration involving a rural community college that offers a Bachelor of Applied Science degree in applied business information and technology (ABIT) with a certification in cybersecurity to seven high schools. This collaboration involves the dissemination of an outreach out-of-school (i.e., after-school program) early college cybersecurity career pathway to high schools with limited or no formal cybersecurity education.

Chai, Bagchi-Sen, Goel, Rao and Upadhyahya (2006) claim that underrepresentation of the minority workforce in the information technology (IT) industry is one of the reasons for the scarcity of skilled labor in the information security industry. Funded by the National Science Foundation Scholarship for Service National Science Foundation (NSF) Scholarship for Service (SFS) [Award #1516178 (10/15/2015–09/30/2017)], this two-year study is designed to increase the number of minorities and women succeeding in college-level cybersecurity education and degree programs by offering a Cybersecurity Certificate of Competence as highlighted in Table 1.

TABLE 1: University of Hawaii Maui Campus (UHMC) Cybersecurity Certificate of Competence Courses (Total 12 credits)

Fall Semester	Spring Semester	Summer Semester
	Spring 2016 - Courses ICS 101 & ICS 110	**Summer 2016 - Courses** ICS 101 & ICS 169
Fall 2016 - Courses ICS 101, ICS 169 & ICS 184	**Spring 2017 - Courses** ICS 101, ICS 169, ICS 184 & ICS 171	**Summer 2017 - Courses** ICS 101 & ICS 171

The following is the listing of the information computer science (ICS) courses and their descriptions for the Cybersecurity Security Certificate of Competency.

- ICS 101—Digital Tools for the Information World: Emphasizes production of professional level documents, spreadsheets, presentations, databases, and web pages for problem solving. Includes concepts, terminology, and a contemporary operation system.
- ICS 169—Introduction to Information Security *(Prerequisite: ICS 101 with grade C or better, or consent)*: Provides the basic foundation for information security, including identifying threats, planning for business continuity, and preparing for various security attacks. Focus will be given to threats to financial security such as attacks on banking and other related financial information. Special emphasis on ethics and legal issues that cover hacking and other cybersecurity techniques and tactics
- ICS 184—Introduction to Networking *(Prerequisite: ICS 101 with grade C or better, or consent)*: Provides the student with the knowledge and skills to manage, maintain, troubleshoot, install, operate, and configure basic network infrastructure, as well as to describe networking technologies, basic design principles, and adhere to wiring standards and use testing tools.
- ICS 171—Introduction to Computer Security *(Prerequisite: ICS 101 or consent)*: Examines the essentials of computer security, including risk management, the use of encryption, activity monitoring, intrusion detection, and the creation and implementation of security policies and procedures to aid in security administration.
- Highly Recommended - ICS 110—Introduction to Computer Programming *(Prerequisite: ICS 101 with grade C or better, or consent)*: Teaches fundamental programming concepts including sequential, selection, and repetition flow; variables and types; syntax; error types; compilation; linking; loading; and debugging. Introduces algorithms flow charts, UMI, and other analytic tools. Explains and offers practice in problem solving and critical thinking methods.

The NSF SFS grant pays for university tuition, fees, and textbooks, as well as a recruiter-agent, faculty, student mentors, and an evaluator. Students earn college credits while they are still attending high school. With a high proportion of diverse and non-traditional students enrolled in rural community colleges, schools have a critical outreach role in expanding access to cybersecurity careers. Research in economic human capital and signal theories (Baptiste, 2001; Spence 1973) imply cybersecurity is a viable college/career choice for students.

The project goals translate to the measurable outcomes listed below in Table 2.

TABLE 2: Proposed Quantitative Measure of Project Success and Examples of Target/Total/%

#	Outcome Measure	Target	Total	%
1	Number of students participating	Year 1: 24, Year 2: 48	72	100%
2	Number of students completing the program	Year 1: 20, Year 2: 40	60	83%
3	Number of students from under-represented populations, including women, Native Hawaiians and Pacific Islanders	Year 1: 8, Year 2: 16	24	33%
4	Number of students continuing in internships (paid/unpaid) or securing a job beyond the program	Year 1: 8, Year 2: 16	24	33%
5	Number of students who continue or elect further education in cybersecurity programs at UHMC or other higher education options	Year 1: 20, Year 2: 40	64	83%

What can we say about the role of community colleges and the demand for cybersecurity skills? This key question for rural communities is central to uncovering promising practices that sync community colleges and high school career and technical programs to develop, expand, and strengthen cybersecurity career pathways.

FIRST REFLECTIVE ACTION: WHAT IS THE CONTEXT?

The University of Hawaii Maui College (UHMC) is a rural hybrid college. It is the only college offering both bachelors and associate degrees in the ten-campus University of Hawaii (UH) system, which includes seven community colleges and three universities.

Through its varied degree and certificate options, UHMC addresses the needs of a diverse student population of approximately 4,000 students in a three-island community with its main campus located in Kahului, Maui. UHMC outreach education centers are located on Maui in Hana and Lahaina. The islands of Molokai and Lanai have an estimated population of 154,834 (as of the 2010 U.S. Census). Over 10% of the population consists of Native Hawaiian and other Pacific Islanders. Their percentage is much higher in the more remote locations such as Molokai and Hana—26% and 29%, respectively (Maui County Data Book, 2012). High schools in these areas lack access to basic technological services and certified technically trained teachers.

UHMC is progressing in its cybersecurity workforce development efforts. As a statewide P-20 centralized system, the study's sustainability plan is to: (1) align with Hawaii's dual enrollment public policy; (2) partner with the P-20 early college initiative; and (3) collaborate with the University of Hawaii Community Colleges U.S. Department of Labor workforce development initiatives in developing a two-year cybersecurity career pathway that aligns with Hawaii's high school Career and Technical Education (CTE) career pathway system. Table 3 outlines the study's iterative timeline and student cohort deployment process.

TABLE 3: Iterative Deployment Process

Round 1 – Spring 2016 (Student Cohort 1)
Round 2 – Summer 2016 (Student Cohorts 1 and 2)
Round 3 – Fall 2016 (Student Cohorts 1 and 2)
Round 4 – Spring 2017 (Student Cohorts 1 and 2)

Data is being collected from student pre-surveys, institutional documents, and observations of participants. The project deployed its Student Cohort 1 in spring 2016 by offering two Information Computer Science (ICS) classes via e-learning technologies (i.e., online courses): Information Computer Science 101 (ICS 101) and Information to Computer Science 110. Students in the project volunteered after attending an open-house on cybersecurity education at UHMC and high school class presentations. The demographics of Student Cohort 1 are highlighted in Table 4.

TABLE 4: Student Cohort 1 Demographics

Description	Number of Students
Grade 11	13
Grade 12	28
Males	13
Females	28
Part Hawaiian	2
Filipino	20
Caucasian	3
Hispanic	1
Japanese	2
Thai	1

As of summer 2016, the project is deploying Information to Computer Science 169 (ICS 169) to Student Cohort 1 and has established Student Cohort 2 by offering ICS 101. This early college cybersecurity outreach option seeks to broaden access to cybersecurity courses through out-of-school learning environments located at high schools.

SECOND REFLECTIVE ACTION—WHAT DID WE LEARNED?

High school women and minorities involved in early college outreach options are uniquely positioned to offer signals and candid insights because of their marginalized access to high school or college credit cybersecurity education. What can we learn from high school students about early college outreach cybersecurity career pathway options? During the study's initial stage, we learned the following: 1) what excites students about attending UHMC early college cybersecurity option; 2) what are potential barriers to online learning; and 3) how to orchestrate resources to create a network.

Initially, Student Cohort 1 (41 students) was asked on a pre-assessment survey, "What excites you about attending UHMC as an early admit student?" Figure 1 highlights their responses. Spring 2016 semester students (41 high school students) illuminate points of intersection across interest and convergence of activities. The areas closer to the center of the web represent a higher the rank of choice. These include, more information about what the jobs might entail; access to more relevant classes to see if I would be good in; reassurance that I would earn a good living; and opportunity to speak to current professionals about the pros and cons.

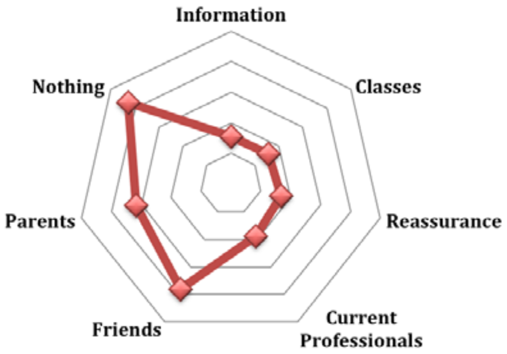


Figure 1. What excites you about attending UHMC as an early admit student?

Next, through monitoring our actions and students' online engagement, we discovered that the e-learning technology platform were not accessible at various high school campuses. Moreover, we discovered that students were having difficulties navigating the e-learning technology management platform. A UHMC recruiter-agent was partnered with a student peer mentor and conducted outreach support to address the students' learning challenges in a timely, face-to-face manner at the high school campuses.

A number of women and minority students were unable to even ask the right question or self-advocate for their learning needs in a digital environment. Thus, parent orientations and hands-on lab sessions are currently being implemented at the beginning of each semester. Additionally, the recruiter-agent collaborated with the faculty in monitoring students' online course engagement to address e-learning instructional challenges.

Finally, to facilitate deep-relationship building across educational sectors, the recruiter-agent actively plans and leads appropriate outreach activities involving high school teachers and staff to discover and learn alongside students about technology and e-learning methodologies and/or platforms within a collective (i.e., an outreach network) learning environment. The following are questions that facilitate the collective's learning process.

Stakeholders: Who are the major stakeholders? How are these stakeholders organized structurally (i.e., departments, career pathways, programs, master schedules, calendars, etc.)? How we access information and share resources? How do we communicate and make decisions?

Students (Women and Minorities): Where and how do we recruit the women and minorities? What are the essential connecting activities women and minorities require that support their resilience and entry into cybersecurity careers? How do we navigate and interface across educational sectors to align human capital and share resources that support equity for women and minorities entering cybersecurity college programs?

The initially findings appear to be positive; all of Cohort 1 students successfully passed the first ICS 101 or ICS 110 course. Then again, as leaders, we need to blur our institutional boundaries by collectively learning how to share resources, risks, responsibilities, and rewards across educational sectors.

THIRD REFLECTIVE ACTION – HOW WILL WE CONTINUE TO KNOW?

As part of the study's reflective iterative process, this section shares the use of an iterative process to discover integrative ways to engage a broader, more diverse group of students in cybersecurity. The initial insights from this case study use a conceptual framework—namely, Kemmis and McTaggart (2005)—an iterative action research process adapted from Lewin's Action Research Cycle, as illustrated in Figure 2. Iterative Action Research Process.

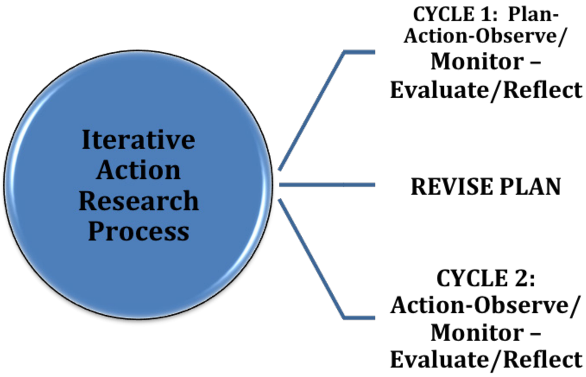

Iterative Action Research Process
CYCLE 1: Plan-Action-Observe/ Monitor – Evaluate/Reflect
REVISE PLAN
CYCLE 2: Action-Observe/ Monitor – Evaluate/Reflect

Figure 2. Iterative Action Research Process, adapted from Lewin's Action Research Cycle [Kemmis and McTaggart (2005)]

Adopting a relational stance allows us to see how different forms of knowing and different forms of interests are integrated as well as how conceptual categories may be turned into living practices where people offer real-life explanations for what they are doing (McNiff, 2013). Moreover, according to Whitehead (2010) knowing becomes a real-life practice; the boundaries between theory and practice becomes a form of "living theory." This action research paradigm allows us to continuously improve in this small-scale project by: (1) shaping the role of community college in early college outreach cybersecurity options; (2) developing a high school student baseline for cybersecurity education in a rural community; and (3) providing effective perspectives on and strategies for leaders in the field.

Overall, by crossing educational sector boundaries (i.e., high school and higher education) and moving beyond our "ivory tower" it appears that while programming must begin and remain within the institutions, we as leaders must rethink our strategies moving forward in this ever-evolving and demanding cybersecurity workforce. Outreach efforts demonstrate how engaging major stakeholders in the high schools and employing site-specific applications of a pre-existing transition model supports internal optimization via external interaction (Penner-Willams, Perez, Worthen, Herrera, and Murry, 2010).

These are the questions we address in this study of women and minorities enrolled: What excites you about attending UHMC as an early admit students? What would increase your interest in cybersecurity career? During high school did any teacher, guidance counselor, career counselor, or other adult in an after-school program or extra-curricular activity ever mention or discuss the idea of a career in cybersecurity? Did/do your high school computer classes offer the skills necessary or prepare you to pursue a career in cybersecurity and/or related degrees like computer science in college? As one woman stated, "New classes. Access to relevant classes to see if I would be good at it would increase my interest in cybersecurity careers."

Because high school schools may not offer any computer science our cybersecurity courses, another woman stated: "[The] opportunity to speak to current professional about the pros and cons would increase my interest in cybersecurity career. I didn't take any high school computer classes to offer the skills necessary or prepare me to pursue a career in cybersecurity and/or related degree like computer science in college." Similarly, another women answered, "No, my high school does not have any computer classes. I would increase my interest in cybersecurity career, if I had access to more relevant classes."

Thus, the initial findings of women and minorities accessing cybersecurity education has provided us with insights by employing an iterative research process which allows us to develop new outreach strategies for collaboration across educational sections in a timely manner. Our intention is to highlight the challenges inherent in today's educational systems and to encourage leadership based on learning and collaborative practices.

CONCLUSION

There is a lack of formal sequenced cybersecurity courses and/or programs in rural high schools. With a high proportion of diverse and non-traditional students enrolled in rural community colleges, these institutions have an outreach role in expanding access to cybersecurity education and careers. Community college outreach may serve as the critical bridge to address the persistence of women and minorities in cybersecurity careers.

Arguably, knowing the complexities and challenges that early admit poses has never been as important due to the increasing need for the community colleges to provide trained workers for the cybersecurity workforce. The barriers may be formidable but so are the community college leaders working to make a difference for students and their communities via their outreach roles.

REFERENCES CITED

Baptiste, I. (2001). Pedagogical implications of human capital theory. *Adult Education Quarterly*, 51(3), pp. 184–201.

Bragg, D. D. (2013). Career and Technical Education: Old Debates, Persistent Challenges in Community Colleges. In Levin, J. S. and Kater, S. T. eds. *Understanding Community Colleges*. pp. 187–202. New York: NY: Routledge.

Chai, S., Bagchi-Sen, S.; Goel, R., Rao, H. R., and Upadhyaya, S. (2006). *A Framework for Understanding Minority Students' Cyber Security Career Interests*. Proceedings of the 12th Americans Conference on Information System, Acapulco, Mexico.

Kemmis, S. and McTaggart, R. (2005). Participatory Action Research: Communicative Action and the Public Space. In Denzin, N. K. and Lincoln, Y. S., (eds.). *The Sage Handbook of Qualitative Research*, 3rd ed., pp. 271–330. London: Sage Publications

Maui County Data Book. (2012) Retrieved September 16, 2013, from http://hisbdc.org/BusinessResearchLibrary/MauiCountyDataBook2012.aspx.

McNiff, J. (2013). *Action Research: Principles and Practices*, 3rd ed. New York: NY: Routledge.

Morest, V. S and Karp, M. M. (2006). Twice the Credit, Half the Time? The Growth of Dual Credit at Community Colleges and High School. In Bailey, T. and Morest, V.S., eds. *Defending the Community College Equity Agenda*, pp. 223–245. Baltimore, MD: Johns Hopkins University Press.

Osterman, P. (2012). The Promise, Performance, and Policies of Community Colleges. In Wildavsky, B., Kelly, A.P., and Carey, K., eds. *Reinventing Higher Education: The Promise of Innovation*, pp. 129–158. Cambridge, MA: Harvard Education Press.

Penner-Willams, J., Perez, D., Worthen, D. G., Herrera, S., & Murry, K., 2010). A CLASSIC Approach to Collaboration: Documenting a Multi-State University and Multi-School District Partnership. In Slater, J.J. and Ravid, R., eds. *Collaboration in Education*, pp. 161-167. New York, NY: Routledge.

Spence, M. (1973). Job marketing signaling. *The Quarterly Journal of Economics*, Vol. 87, No. 3. (Aug., 1973), pp. 355–374. Retrieved from: http://www-bcf.usc.edu/~shaddin/cs590fa13/papers/jobmarketsignaling.pdf.

Whitehead, J. (2010). As an educator and educational researcher, how do I improve what I am doing and contribute to educational theories that carry hope for the future of humanity? Inquire in Education 1(2), Article 2. Retrieved from: http://digitalcommons.nl.edu/ie/vol1/iss2/2.

AUTHOR

Debra A. Nakama, PhD, (debran@hawaii.edu) is the vice chancellor of student affairs at the University of Hawaii Maui College (UHMC). Nakama is the principal investigator for National Science Foundation (NSF) Scholarship for Service (SFS) study: Addressing the Need for Women and Minorities in Cybersecurity: A High School Early Admit Study [Award #1516178 (10/15/2015–09/30/2017)], a two-year study designed to increase the number of minorities and women succeeding in college-level cybersecurity education. She has more than two decades of experience in using collaborative systemic strategies with stakeholders for increasing the college transition rates of underachieving and under-represented students.

EXCELSIOR COLLEGE

FOUNDED IN 1971