Promising Practices for Building Cybersecurity Knowledge, Confidence and Capacity among College Professors

Monique Jethwani
Mmj2106@columbia.edu

Nasir Memon
nm1214@nyu.edu

Columbia University School of Social Work
1255 Amsterdam Avenue
New York, NY 10027 USA

New York University Tandon School of Engineering
Computer Science and Engineering
2 MetroTech Center
Brooklyn, NY 11201 USA

Abstract- There has been increasing awareness that any scalable and sustainable effort to grow the workforce in cyber security cannot focus only on university students, but also college professors. Many are looking to higher education to produce skilled and capable cybersecurity professionals but little is known about what these professors really need. Utilizing data gleaned from focus groups and surveys with college and university computer science professors (N=30) that participated in a cybersecurity professional development program at a leading urban university, this research aims to identify promising practices for building cybersecurity knowledge, confidence and capacity among college professors. Results indicated that the participating computer science professors had experience with cybersecurity but were not confident in their teaching skills in this area. Participants reported that the hands on and applied activities in the professional development training supported both knowledge and confidence building. They attributed their capacity to build coursework at their respective institutions to the materials provided during the professional development. However, findings also suggest that without ongoing mentorship, collaboration and diversity training, capacity

building might be limited. These results contribute to a greater understanding of evidence based practices with college professors in cybersecurity.

Keywords

Cybersecurity, Qualitative, College Professors, Education

1. INTRODUCTION

According to the US Department of Education (n.d.), technology related jobs are projected to increase 22-32% between 2010 and 2020. The White House (2016) reports that computer science has become "a basic requisite for 21st century jobs" and there could be 2.4 million unfilled STEM related jobs by 2018. Governments and organizations world-wide are expressing concern about a cybersecurity skills crisis. A study by Cisco estimates that approximately 1 million security professional positions are currently vacant (ISACA, 2014). Others report that approximately 70% of security organizations are understaffed and 50% of all leadership roles are unfilled (Rosenquist, 2015). Cybersecurity attacks threaten all sectors, facets and aspects of American society, making it essential that we find ways to prepare all of our citizens for work in the digital world (Shoemaker, 2014).

There is increasing concern that higher education is ill equipped to meet this growing need for cybersecurity professionals. One study found that 47% of college students who plan to pursue careers in cybersecurity do not feel they have enough knowledge in cybersecurity to meet the demands of a job in the field, and 23% report that their university does not offer courses in cybersecurity (ISACA, 2014). And with only 18% of computer and information sciences undergraduate degrees earned by women (NCWIT, 2012), there are simply not enough people to fill the gap.

There is an urgent need to educate a diverse population of computer scientists to analyze and defend against cyber-attacks. There has been increasing awareness in the academic community that any scalable and sustainable effort to grow the workforce in cyber security cannot focus only on university students, but also

college professors (National Public Radio, 2010; Office of Press Secretary, 2009). Many are looking to higher education to produce skilled and capable cybersecurity professionals that will be able to defend our networks and infrastructure. However, many college faculty do not have the required background to teach cyber security courses, or to mentor students in related research (Rosenquist, 2015). "Academic structures are not well aligned to the needs of the industry, there is a lack of consistent degree and curriculum standards, and educating students with relevant content, in a rapidly changing field, is proving difficult with traditional practices" (Rosenquist, 2015). The President's Council of Advisors on Science and Technology (2012) identified the need to support greater innovation in STEM undergraduate education.

It is essential that community college and liberal arts college faculty engage in cyber security teaching and research experiences so that they may build the knowledge they need to confidently prepare the next generation of cyber security professionals. However, little is qualitatively known about how professors experience and define the challenges to building a cybersecurity workforce. Utilizing data gleaned from focus groups and qualitative surveys with college and university computer science professors (n=30) that participated in a cybersecurity professional development program at a leading urban university, this research aims to understand what computer science professors need to build their cybersecurity knowledge and confidence.

1.1 Research Question:

- What do college professors need to build their knowledge, confidence and capacity in cybersecurity?

In this paper, section two provides a description of the procedures and data collection and analysis methodologies used in this study; section three documents the results of the study and section four offers conclusions, including the limitations of this study and suggestions for future research.

2. METHOD

2.1 Sample

Thirty computer science professors from twenty-eight different colleges and universities nation-wide, representing 18 states/ territories, participated in this research. Twenty percent of these participants were female, which is reflective of female representation in the computer science field (NCWIT, 2012). Of the 30 participants in this study, 50% identified as East and South Asian; 16.7% White; 20% Black/ Latino; and 13.3% Other.

2.2 Setting

Participants were taking part in a project, funded by the National Science Foundation, that aimed to create awareness, proficiency, and innovation in the area of cybersecurity among the US two-year and four-year college community. All participants in this project (N=30) over a period of three years participated in this study and signed assent forms indicating their participation. As a part of the project, professors from colleges and universities nation-wide participated in professional development and a collaborative research project. The two week professional development program exposed participants to fundamentals of cyber security using lectures, hands-on experiences, and discussions of topics related to the security of operating systems, networks and applications. Participants got involved in research projects that explored topics such as biometric identification systems, the security of database application programs, the cyber defense of WiFi enabled physical devices and understanding virtualization through reference monitors. Participants then adapted components of the structured training they received to create material for courses activities in their home computer science departments. Modules included topics such as biometrics, authentication techniques, SQL and database application programming, web application security, VHDL modeling, assessing vulnerabilities in digital designs and hardening FPGA designs to detect Trojans, Cyber forensics and cyber defense for mobile phones and Security and virtualization.

2.3 Data Collection

2.3.1 Surveys (N=25/30)

Participants in the project completed a short survey after the professional development component of the project. This survey included demographic information (gender, ethnicity, teaching experience) and Likert scale items. With responses that ranged from disagree a lot to agree a lot, these scale items explored participant's experiences in, and confidence with teaching cyber security and how participation in the program supported their confidence in teaching cyber security and engaging students in CSAW. Some items were selected from the self efficacy subscale of the "Mathematics Teaching Efficacy Beliefs Instrument" created by Huinker & Enochs (1995). Items were revised to reflect teacher self efficacy around cyber security, rather than mathematics. In accordance with Bandura's social cognitive theory, the scale measures the belief that they can teach cyber security effectively. Scores were validated with a sample of 217 college students studying to become teachers (Cronbach's alpha was .81 for the Outcome Expectancy subscale, .89 for the self efficacy subscale and .85 for the overall scale). In this evaluation, six items were removed from the self efficacy subscale in order to minimize the fatigue of our respondents. Participants also responded to fill in questions where they reflected on their likes and dislikes about the professional development they received and their plans for integrating cyber security into their school communities.

2.3.2 Focus groups (N=20/30)

Focus groups provide opportunities for insightful and contextual discussions about pertinent issues in individuals' lives and are viewed as helpful in understanding how stakeholders regard specific experiences (Massey, 2011). Questions explored participants' experiences in the project, their experiences with teaching cyber security, their thoughts about integrating cyber security courses and programming at their home colleges and their ideas for how the professional development or research components of the project might be improved for future participants. Focus groups were held in private rooms and recorded with the permission of the

participants. One of the co-authors of this paper, a trained qualitative researcher and developmental psychologist, conducted the focus groups.

2.3.3 Annual progress reports (N=19/30)

Participants reflected on their accomplishments and experiences in the following areas: teaching, networking, research, publications, and competition involvement.

2.4 Data Analysis

First, frequencies were calculated for each of the survey items to determine perceptions of self-efficacy. Second, qualitative methodologies were utilized to analyze the focus groups, narrative responses on surveys and end of year reports. This analysis relied upon the qualitative methodology of open coding; a strategy that divides the narrative data into discrete units of analysis (quotes) reflective of the major themes that are embedded in the words of study participants (Miles & Huberman, 1994).

Verbatim transcripts (amounting to more than 100 transcribed pages) were read multiple times by a research team consisting of the lead evaluator and three graduate students to combat reliability and validity threats. Then, a coding scheme was developed to identify where, when and how often the professors discussed various themes. This approach aims to "understand the complex world of lived experience from the point of view of those who live it" (Schwandt, 1988, p.221). The coding scheme represented the emergent themes identified in the initial read-through of the transcripts, surveys and final reports (i.e. ideas for improvement) and variables of interest including barriers and strengths of the summer program and research projects, attitudes and beliefs about computer science, program engagement and fidelity, and experiences creating teaching modules or other activities. See Figure 1 for examples of codes and their definitions.

Finally, all of the data (quotes) assigned to each code were reviewed to identify overlapping patterns across data sources. Matrices were created to summarize, consolidate and organize the central themes that revealed professors experiences that were described by a majority of the participants. Themes are presented in this paper

with illustrative quotes drawn from the focus group texts (in italics), staying true to the language of both the participants and the interviewer.

Code	Definition	Examples
CONFIDENCE/ SELF EFFICACY	Feelings of confidence in teaching cyber security both before and after the summer program	"I found the summer program to be very useful and it definitely provided me with new tools to use in my classroom."
RESEARCH PROJECT	Thoughts about the research project participants would be undertaking with their mentors. Both positive and negative.	"I actually want to start collaboration. I don't want to finish a project within these four weeks and forget about it."
SUMMER POSITIVES / CHALLENGES ** This code was used in first round of coding. Once positives and negatives were identified, the data was re-coded for these themes (i.e. 'hands on activities' or 'simplified content')	Reflections on most positive and most challenging aspects of the summer program	"Their strategy during the summer program was to try to cover as much as possible, but I think it would have been beneficial to go the other way. Cover very few topics, maybe just one activity per session, but provide more explanation."

Figure 1: Sample from Code Book

3. RESULTS

3.1 Professional development with hands on and applied activities builds confidence

Seventy-two percent of participants agreed[1] that they knew a lot about cyber security prior to participating in the summer program. However, only 28% agreed that they would, given the choice, invite their Dean to evaluate their cybersecurity teaching, suggesting low feelings of self-efficacy in this area. Participants reported that the training and professional development received successfully built their confidence. Ninety-six of participants agreed that after participating in the summer training program, their confidence in their cyber security skills increased. See Figure 2.

[1] Of the twenty five participants that completed surveys at the completion of their participation in the summer training program.

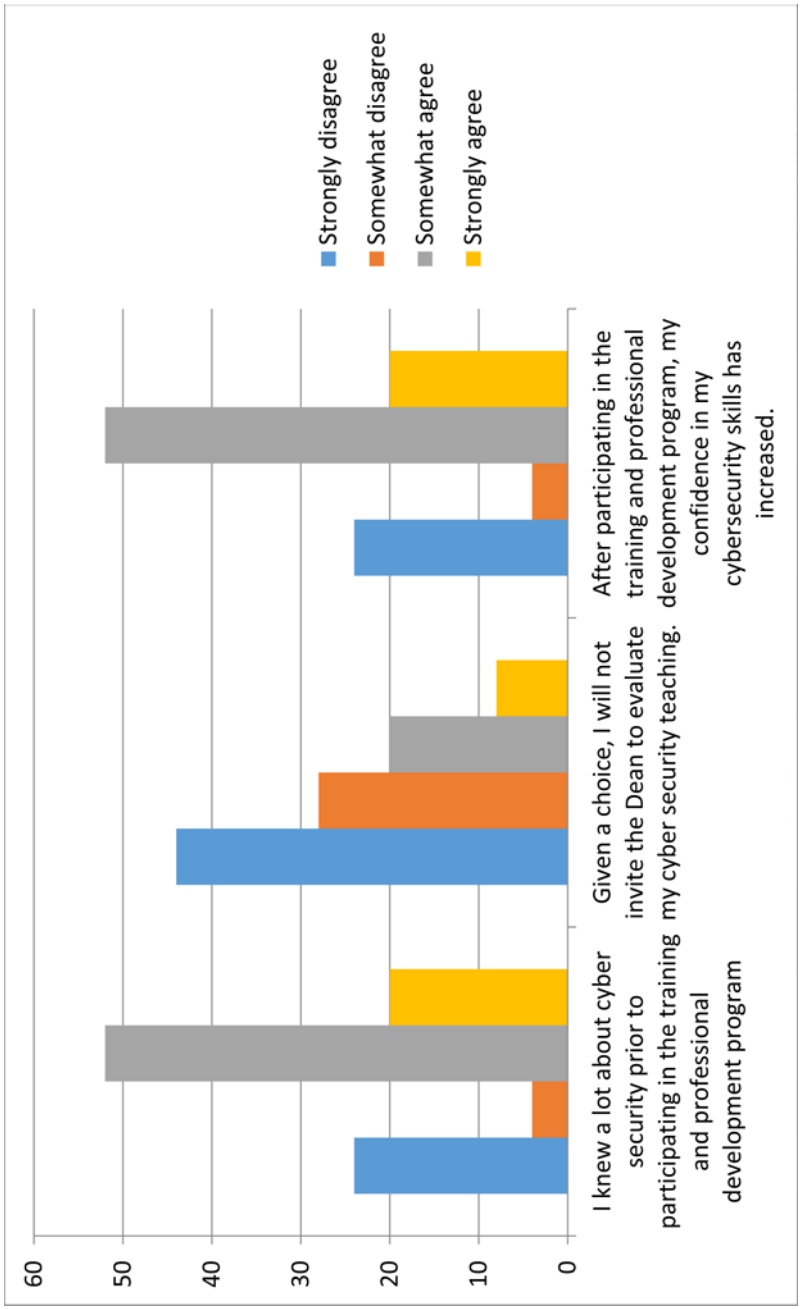

Figure 2: Prior knowledge and confidence frequencies

The qualitative data in this study (focus groups and fill in responses) also revealed evidence of improved confidence in their cybersecurity knowledge and teaching skills. One participant explained that although "*Some of the topics were way above my level of experience, knowledge and expertise*" he felt more confident in his skills and better prepared to teach and mentor his students in topics related to cybersecurity as a result of his participation. Another participant stated,

> *I feel more confident because I think before I was interested, but I didn't know where to start to learn about these things. But now I feel like I know. The exposure helped me to learn about resources that have been made available and I know where to go.*

Faculty went on to introduce students to concepts and challenges in cyber security via courses, modules, clubs, labs and competitions in their own colleges and universities. Newly created cyber security/ network forensics courses and modules included: Architecture and web design; Computer hardware and software; Analysis, design and implementation of information systems; Memory corruption; Host exploration; Buffer overflow; Data imaging using windows tools; Forensics analysis; Investigating windows systems; Steganography; Email tracing; Worm and virus analysis; Applied cryptography; Penetration testing; Firewall and Seattle exercises; Python programming; Caesar Cypher; Password strength and Benford's Law. For example, the following two assignments were developed for an undergraduate Operating Systems course in Ohio.

a. *Develop a Reference Monitor inside of an API that would prevent MZ from being written to the file (performed in C programming language in MINIX OS)*
b. *Allowed students to "hack" each other reference monitor to see if they could "break it". For this, I compiled their API source into a library and gave them access to each other's library for compilation into their test programs.*

Another professor reported that his students experienced "*Greater achievement and engagement in cybersecurity and new appreciation of security features in Operating Systems.*" He explained;

> *In the Fall semester, I developed two teaching modules on the issues of malicious circuit insertion, also known as Trojan circuits, for my FPGA Design class. The first module*

introduced the goals and challenges of attaining hardware security, presented a taxonomy of Trojan circuit classifications, and discussed some methods used to detect Trojans. A case study of hardware Trojans developed for a wireless encryption circuit was undertaken. The second module went into more detail on how to detect Trojans, covering such concepts as parametric testing and IC fingerprinting.

Another professor explained how the summer program helped him to develop a virtual lab for security education at his university and to revise his curricula to better meet NSA expectations;

As a designated center for Academic Excellence in Information Assurance/ Cyber Defense, we are now working on revising our security curriculum to meet the national/ regional demands. Motivated by the presentations on variant cyber security courses from the summer program, we are revising our current curriculum on cyber security, including undergraduate and graduate courses.

Participants attributed their increase in knowledge and confidence in cybersecurity, and their capacity to build coursework at their respective institutions, to the hands on and applied activities and materials provided during the summer program. "*Examples from the lectures, lab exercises, some of the software developed, and the resources shared with us are all very useful in preparing for these classes.* These findings together suggest that hands on training and professional development in cybersecurity is associated with knowledge and confidence building among computer science professors, leaving them better prepared to train a new and diverse cybersecurity workforce. However, findings suggest that without ongoing mentorship, capacity building might be limited.

3.2 Building resources for cybersecurity in higher education via collaboration and mentorship

Many of the participants, especially those from small, non-research, institutions, explained that they do not have the resources or the facilities necessary to meet student demand for cybersecurity courses and activities, or to develop and fund cybersecurity research projects.

We are financially constrained to provide tools and resources to our students so even though we see that there are a lot of talented students coming to our school, we're not really satisfying their need and this I think causes a big problem in the retention and also not producing quality workforce after the four years of their study at the institution… Small colleges usually do not have resources and facilities to satisfy all the demand so if there is any way we can share any teaching tools or facilities that would be a great benefit for us and hopefully we can also benefit a bigger institution by presenting their teaching tools and facilities to our students.

In addition to teaching tools, many professors were unsure how to secure the resources needed to sustain their research interests

One of the eye-opening experiences that I've had is to realize that bigger institutions that have more financial resources are likely developing programs and they can also keep up with the pace of the fast moving industry. Whereas small institutions, they are more tuition driven. We are financially constrained to provide tools and resources to our students so even though we see that there are a lot of talented students coming to our school, we're not really satisfying their need and this I think causes a big problem in the retention and also not producing quality workforce after the four years of their study at the institution. So I think there should be some way to create partnerships or collaborations.

Collaborations are likely to support the sustainability of cybersecurity courses and activities in computer science departments nation-wide, which would support the education of more cybersecurity professionals. This collaboration might also support efforts to engage a more diverse workforce.

3.3 The need for diversity training and female mentors

Professors agreed that there is a strong lack of female representation in their computer science courses and many admitted that they did not know what to do to turn girls on to cybersecurity. When asked to reflect on their efforts of recruiting more female students in the computer science departments at their respective institutions, professors offered some insight into the subtleties of gender discrimination in higher education. Some participants questioned if computer science was an "appropriate field for women" due to the long hours, their level of

skill or the "social tension" that their presence would create. For example, when asked to identify ways in which they might recruit more females at their respective institutions, one college professor stated;

Would it be beneficial to the society? Just joking because if females know how to understand cyber security I think they'll be more social tension, no? Off the record please.

Jokes such as these are likely to contribute to lack of female representation. Another professor explained that girls' tendencies to be 'detail oriented' might make them 'superior' to boys in 'some areas' but the amount of time that one has to dedicate to work, and away from family, might be an obstacle for girls and women.

I have found that cybersecurity is a broad area and there are multiple disciplines in this industry and there are some areas female students can be superior. For instance software security because the way they think is very detail oriented so if we can present some of the existing software that people think are quite trustworthy are not and they have a lot of loopholes and there is a chance for female programmers or somebody who can investigate those loopholes further and come up with solutions then I think you will give them more confidence and give them opportunity. Otherwise, I think this industry is somewhat difficult for females because even some of the instructors who showed us some hands on, they bluntly say they are working all night and then they usually do not work during the day so I do not know how that will fit into both genders.

Some admitted to a concern that bringing in too many females would jeopardize the 'quality' of students.

I think on the same note it's important not to overdo it where just to get females you forget about quality and just bring 50% of not males and then it's kind of promoting the stereotype of them being incompetent… What I'm saying is don't create artificial quotas.

Female mentorship and diversity training might offer support to female faculty and students and also help to develop more male allies. As girls find themselves minorities in the classroom, they feel as though they must "work harder" to counteract this discrimination and change perceptions about their skill, ability, and their place in computer science (NCWIT, 2012; Williams, Phillips & Hall, 2014).

These experiences challenge girls' confidence (Shapiro & Williams, 2012) even though, with similar training and experience, girls and boys perform at comparable levels in computer science (Aronson, Quinn & Spencer, 1998). One of the two female participants in this project explained the importance of building confidence in what can often be a hostile environment for females.

I think something that needs to be done. I don't know it probably needs to be done sooner than just when you get to undergraduate, is confidence building. Because, guys, they just think they're right all the time even though they're not and women always doubt themselves. This is a recurring theme and you just see it. And when you have a lot of males in the same group, aggressiveness comes out which makes it less appealing for women. Being one of the few faculty, I was usually in class with a hundred people and I was a really good student, but still, it's just guys are so much more confident, even if they don't know something. So I think it needs to be somehow ingrained in women, that they can do it.

Another participant explained that opportunities to get girls 'up to speed' in terms of their experience with cybersecurity would build confidence.

I think what scares some girls away from computer science is the gap between many male students that have spent hours and hours hacking before they come into the university versus them that just basically are starting to learn about computer science. I think a way that we in colleges can contribute to this is having classes where we get them up to speed- to bridge the gap where they can exchange ideas with people like the presenters today.

Diversity training and female mentorship are likely to both support female faculty and recruit female students (NCWIT, 2012).

4. CONCLUSIONS

Results indicated that the participating computer science professors had experience with cybersecurity but were not confident in their teaching skills in this area. Participants reported that the hands on and applied activities in the professional development training supported both knowledge and confidence building. They attributed their capacity to build coursework at their respective institutions to the

materials provided during the professional development. However, findings also suggest that without ongoing mentorship, collaboration and diversity training, capacity building might be limited.

In order to ensure a qualified, diverse and plentiful cybersecurity workforce, it is essential that we engage more college professors in the field (Rosenquist, 2015). This qualitative study was undertaken in an attempt to explore the following research question: What do computer science college professors need to build their knowledge and confidence in cybersecurity? This study was unique in its' emphasis on perceptions of cybersecurity among computer science professors and in its' attempt to identify the ways in which subtle changes in the social context can enhance professors' confidence in their cybersecurity skills. The results of this study suggest that professional development in cybersecurity that offers hands on and applied activities can effectively bolster confidence among computer science professors. This study also revealed that college professors might benefit from ongoing collaboration with, and mentorship from, other more experienced computer science professors. Because there is not a nationally recognized degree in cybersecurity, graduates enter the workforce with vastly different security skills. Mentorship and collaboration is likely to support the capacity for ongoing cybersecurity courses and research projects that prepare students for the rapidly changing industry (Rosenquist, 2015). It is also essential that efforts be made to attract women and ethnic minorities to the field. This study identifies the need for more female-friendly environments in higher education computing contexts.

4.1 Women in cybersecurity

In order to protect the world's economy and security, there is a growing need for cybersecurity professionals trained in areas related to network security, risk mitigation and information protection. However, there is a severe shortage of cybersecurity specialists in the US and in many locations worldwide (Shumba et al., 2013). In computer science, computer engineering and information technology, all fields from which cybersecurity draws, women are widely underrepresented (Department of Labor, 2014; NCWIT, 2012). According to the Department of Homeland Security (n.d.) "The lack of women in IT and cybersecurity represents

a failure to capitalize on the benefits of diverse perspectives: in a world dependent on innovation, diversity can bring the best and brightest problem-solvers to the table; and at a time when technology drives economic growth, it can yield a larger and more competitive workforce" (para. 3). However, in order to increase the numbers of females entering cybersecurity fields, we must support female faculty.

Researchers are beginning to explore some of the reasons behind the lack of women in the field of cybersecurity. Some have found that both male and female faculty and professionals in cybersecurity hold gender stereotypes about the field and can identify social and institutional barriers facing women that inform misconceptions about who is entitled to participate (Bagchi-Sen, Rao, Upadhayaya & Chai, 2010; Huang & Bashir, 2015; Shumba et. al, 2013). For example, Bagchi-Sen, Rao, Upadhayaya & Chai (2010) found that the obstacles associated with male-dominated work environments and gender stereotyping leave women feeling that their cybersecurity skills are often underestimated. Huang & Bashir (2015) found that female college students majoring in cybersecurity had lower self-efficacy about their work in the field than their male colleagues, even though there were no gender differences in GPA. Ongoing mentorship and collaboration has been found to support female computer science students and professionals (Williams, Phillips & Hall, 2014).

4.2 Limitations and Future Research

This study contributes to our understanding of best practices for engaging computer science professors in cybersecurity but the generalizability of the results are limited. This study took place in a particular geographic location with a relatively small sample size. Additional data about if and how professors' continue to build cybersecurity capacity at their respective colleges and universities would offer a more complete look at the impact of such practices.

REFERENCES

[1] Aronson J., Quinn, D. & Spencer, S. (1998). Stereotype threat and the academic performance of minorities and women. In J. Swim and C. Stangor (Eds.), *Prejudice: The target's perspective*. Academic Press. p.85-86.

[2] Bagchi-Sen, S., Rao, H.R., Upadhyaya, S. & Chai, S. (2010). Women in Cybersecurity: A study of career advancement. Anaheim, CA: IEEE Computer Society.

[3] Department of Labor (2014). Computer and Information Technology Occupations. http://www.dol.gov/wb/stats/Computer_information_technology_2014.htm

[4] Department of Homeland Security (n.d.). Retrieved from http://niccs.us-cert.gov/home/women-minorities

[5] Huang, H. Y., & Bashir, M. (2015). Examining the Gender Gap in Information Assurance: A Study of Psychological Factors. In *HCI International 2015-Posters' Extended Abstracts* (pp. 117-122). Springer International Publishing.

[6] Huinker, D., & Enochs, L. G. (1995). Mathematics Teaching Efficacy Beliefs Instrument [Database record]. Retrieved from PsycTESTS. doi: 10.1037/t08635-000

[7] ISACA (2014). The growing cybersecurity skills crisis: Addressing the conflict of too many threats, too few skilled professionals. Retrieved April 14, 2016 from http://www.isaca.org/cyber/Documents/Cybersecurity-Report_pre_Eng_0414.pdf

[8] Massey, O.T. (2011). A proposed model for the analysis and interpretation of focus groups in evaluation research. *Program Evaluation and Planning, 34(1),* 21-28.

[9] Miles, M. B., & Huberman, E. M. (1994). *Qualitative data analysis*. Thousand Oaks, CA: Sage Publications.

[10] National Center for Women and Information Technology (2012). Girls In IT: The Facts. Authors: Ashcraft, C., Eger, E. & Friend, M. Retrieved April 14, from https://www.ncwit.org/sites/default/files/resources/girlsinit_thefacts_fullreport2012.pdf

[11] Schwandt, T. (1998). Constructivist, interpretivist approaches to human inquiry. In N. Denzin &Y. Lincoln (Eds.). *The landscape of qualitative research.* Thousand Oaks, CA: Sage Publications.

[12] National Public Radio (2010). Cyberwarrior shortage threatens US security. http://www.npr.org/templates/story/story.php?storyId=128574055

[13] Office of Press Secretary (2009). Remarks by The President on securing our nation's cyber infrastructure. http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

[14] 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. Retrieved April 14, from https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_independence_tech__aging_report_final_0.pdf.

[15] Rosenquist, M. (2015). Higher education must save cybersecurity. Intel Securities Executive Perspectives Blog. Retrieved April 14, 2016 from https://blogs.mcafee.com/executive-perspectives/higher-education-must-save-cybersecurity/

[16] Shapiro, J. & Williams, A. (2012). The role of stereotype threats in undermining girls' and women's performance and interest in STEM fields. *Sex Roles, 66,* 175-183.

[17] Shoemaker, D. (2014). Proceeding of The Colloquium for Information System Security Education. *CISSE, 2 (1),* 4-7.

[18] Shumba, R., Ferguson-Boucher, K., Sweedyk, E., Taylor, C., Franklin, G., Turner, C., Sande, C., Acholonu, G., Bace, R. & Hall, L. (2013). Cybersecurity, women and minorities: Findings and recommendations from a preliminary investigation. ACM ITiCse Conference Working Group, Canterbury, England, UK. http://dx.doi.org/10.1145/2543882.2543883.

[19] The White House (2016). STEM Depiction Opportunities. Retrieved April 14, 2016 from https://www.whitehouse.gov/sites/default/files/microsites/ostp/imageofstemdepictiondoc_02102016_clean.pdf

[20] U.S. Department of Education (n.d.). *Science, Technology, Engineering and Math: Education for Global Leadership.* Retrieved April 14, 2016 from http://www.ed.gov/stem

[21] Williams, J., Phillips, K. & Hall, E. (2014). Double Jeopardy? Gender bias against women of color in Science. Tools for change.