INFORMATION SECURITY RISK AWARENESS PROGRAMS IN K-12: IS THIS THE RIGHT APPROACH?

Syed Raza, Trenholm State Community College; Idong-Mkpong- Ruffin, Faulkner University;
Sajid Raza Walmart Stores, Inc., Bentonville, Arkansas; Ken Scott, Trenholm State Community College

Abstract

In his State of the Union address, President Obama stated that "America must...face the rapidly growing threat from cyber-attacks" [1]. He signed an executive order allowing the U.S. government to share intelligence on potential cyber threats with public and private firms because U.S. schools are not preparing kids for cybersecurity literacy in the digital age [2]. While the Internet has provided powerful tools for education, it also has created risks and raised some improper and unsafe behavior inside and outside of the classroom [3]. In a recent study conducted by Zogby International and released by the National Cyber Security Alliance (NCSA), the data indicated that more than 90% of the more than 1000 teachers, 400 school administrators, and 200 technology coordinators surveyed, noted that they supported the teaching of cyber ethics, safety, and security in schools. However, more than 50% of the teachers indicated that their school districts had no requisite inclusion of these subjects in their respective K-12 curricula [4].

In this paper, the authors propose an awareness program (Cyber-IQ Summer Camp) that should be launched in K-12 to address the need for user awareness about cybersecurity issues. The topic of cybersecurity risks must be introduced early in the curriculum to promote students' understanding of their roles in cybersecurity protection. Since 21st century kids believe that they cannot live without technology, they must understand the implications of security issues [5]. The awareness program through summer camps will build a strong foundation with the motto: "No Child Left Behind in Basic Cyber Security Knowledge"; moreover, students today need to learn strategies to help them understand the concepts of cybersecurity and how to address/apply them—through knowledge, experience, and skills-based activities. Nearly 80% of computer users are becoming victims of fraud and are affected by some type of security threat, due to a lack of awareness about security risks associated with usage of the Internet [6]. A survey conducted by the Ponemon Institute showed that the average cost of cybercrime for U.S. retail stores more than doubled from 2013 to an annual average cost of $7.6 million per company in 2014 [7].

According to an estimate by Morgan [8], a contributing writer with Forbes.com, one million open and unfilled cybersecurity positions were available at the end of 2016, and the predicted cybersecurity service market is anticipated to grow to a $170 billion service industry by 2020. Therefore, technological supply and demand techniques need to be used in order to fill these high-tech positions, presently and in the future. One such highly potential training opportunity is the CyberPatriot program, established in 2009 as an Air Force Association's National Youth Cyber Education Program, designed to motivate students to enter careers in cybersecurity and/or other science, technology, engineering, and mathematics (STEM) disciplines that are critical to our nation's future. In order to expand this initiative in various states, there is a significant need to inform our 21st century digital kids about upcoming cybersecurity demands. To this end, a model program to promote awareness and to encourage K-12 cybersecurity participation has been developed. This program, dubbed the Cyber-IQ Summer Camp, will soon be announced in the K-12 Alabama School System in the River Region, located in Montgomery, Alabama, and participating counties.

Introduction

The aim of this paper is to initiate the first steps towards developing an awareness of and mindset for understanding why cybersecurity is necessary in today's world. The primary focus of cybersecurity awareness is to create and influence the adoption of secure behaviors. This paper is the first in a series of three. Two other papers are expected to follow in which answers about what works, what does not, and why will be identified. Figure 1 shows the developmental model to which this series of papers will subscribe. As indicated in Phase 1, the basic infrastructure has been established. Subsequent to Phase 1, the implementation and data-collection phase will begin, in order to process and report the results in Phase 3.

According to Setalvad [9], in 2015 there were approximately 209,000 cybersecurity jobs vacant, with a trending-up rate of 74% over the past five years in the number of cybersecurity job listings. In other words, there are more cybersecurity jobs open than there are qualified candidates to fill them, and in recent years the media have reported an increase in information security incidents; therefore, President Obama has made information security a national priority [10].

Figure 1. Three-Paper Series Process

Awareness and encouragement about cybersecurity is a skills-based element both in the current K-12 environment and in society in general. Giannakas et al. [11] introduced cybersecurity awareness to K-6 students through an innovative mobile app named CyberAware, in order to educate K-6 students about cybersecurity threats. Another aspect of awareness, named the CyberPatriot program, created by the Air Force Association (AFA), is designed to motivate and inspire K-12 students by delivering basic cybersecurity education and promote STEM [12]; but there is no program directly related to summer initiative programs to promote cybersecurity education for K-12 students.

According to the U.S. Secretary of Defense Ash Carter [13]: "The dominant power of the 21st century will depend on human capital. The failure to produce that capital will undermine American security." Different cybersecurity jobs require more understanding of security or technology; therefore, different avenues need to be developed in order to prepare these digital kids. As previously noted, Butler [3] stated that our district leaders need to take responsibility for teaching students how to wisely navigate the Internet to develop an understanding of cyberworld threats. Therefore, there is a need for strong student participation in cybersecurity activity programs to provide awareness about cybersecurity risks and issues for K-12 students, who will become several generations of cyber-warriors for the U.S.

President Obama [14] stated: "We know hackers steal people's identities and infiltrate private email. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy." For competitive advantage, most business and educational organizations have installed the latest security applications; but, due to a lack of trained staff and users, there is still vulnerability in these respective systems. Hence, to update the organizational infrastructure means nothing if users do not have detailed appropriate awareness and practical skills about cyber safety.

This proposed initiative was designed to provide awareness and encouragement for K-12 students to join Cyber-IQ Summer Camps and obtain a certification of completion; furthermore, this initiative encourages students to join local and state-level programs for Cyber-IQ competitions within and between public and private schools. This process will persuade them to join the cybersecurity field to support President Obama's initiative "... information security [as] a national priority" [14].

Awareness Model

Kortjan and Von Solms [15] stated that in order to reduce computer security risks, training and awareness programs played a vital role in educating individuals. For example, Cyber Portfolio is another attempt to support a cutting-edge methodology for those seeking an innovative approach to integrate technology into curricular lessons [16]; moreover, successful cyber training programs require a substantive technology change in existing curricula throughout a significant number of school districts, with these decisions being supported or avoided by the various Boards of Education.

The Information Security Forum in 2014 [17] and Wilson and Hash [18] with the National Institute of Standards and Standards in Technology, similarly reported that people know the general-nature answers to awareness questions, but they do not act accordingly. Toth and Klein [19], in the NIST Special Publication 800-16, defined awareness as follows: "Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly." Therefore, it is necessary to develop these recognition skills through interactive programs so that the digital kids are not only cognizant of security issues and techniques, but that they are more attuned to the presence of digital intrusions. Figure 2 shows a model of how the process of educating digital kids to the presence of digital intrusions can be accomplished in a step-by-step process. Table 1 defines descriptive identifiers for Figure 2.

The interrelated and interdependent model shown in Figure 2 interacts with and guides students in different workstreams and provides a high-level snapshot of what needs to be done in regards to the cybersecurity process. Instruction through lectures or advice from a person of cyber-authority might set the tone of cybersecurity, but individual knowledge and understanding of cybersecurity are the main influencers on behaviors [20]. Consequently, the main purpose of the awareness model is to establish a competition among K-12 kids about Cyber-IQ. The Cyber IQ-Summer Camp will teach them how to develop secure be-

haviors by passing a set of interactive awareness training activities though different standardized modules with the collaboration of the CyberPatriot Program. (Note: Maxwell Air Force Base Cyber College is located in Montgomery, AL.) Although the Internet has provided powerful educational tools for student learning, it has also created many illegal, inappropriate, and unsafe behaviors among users, especially K-12 students. For teaching the next generation of students about cybersecurity fundamentals, it is required to add knowledge of cybersecurity in all grade levels. Virginia, for example, requires school districts to teach all kids Internet safety and cybersecurity issues for districts receiving certain Federal E-Rate funds; however, this process is not available in all states. The proposed cybersecurity awareness program offers an opportunity to the Alabama School District systems to join Cyber-IQ Summer Camps and participate in Cyber-IQ competitions.

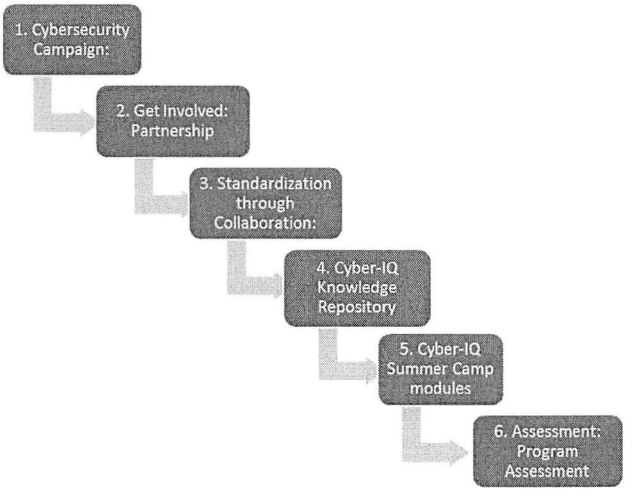


Figure 2. Cybersecurity Awareness Interaction Process

Security Awareness Programs

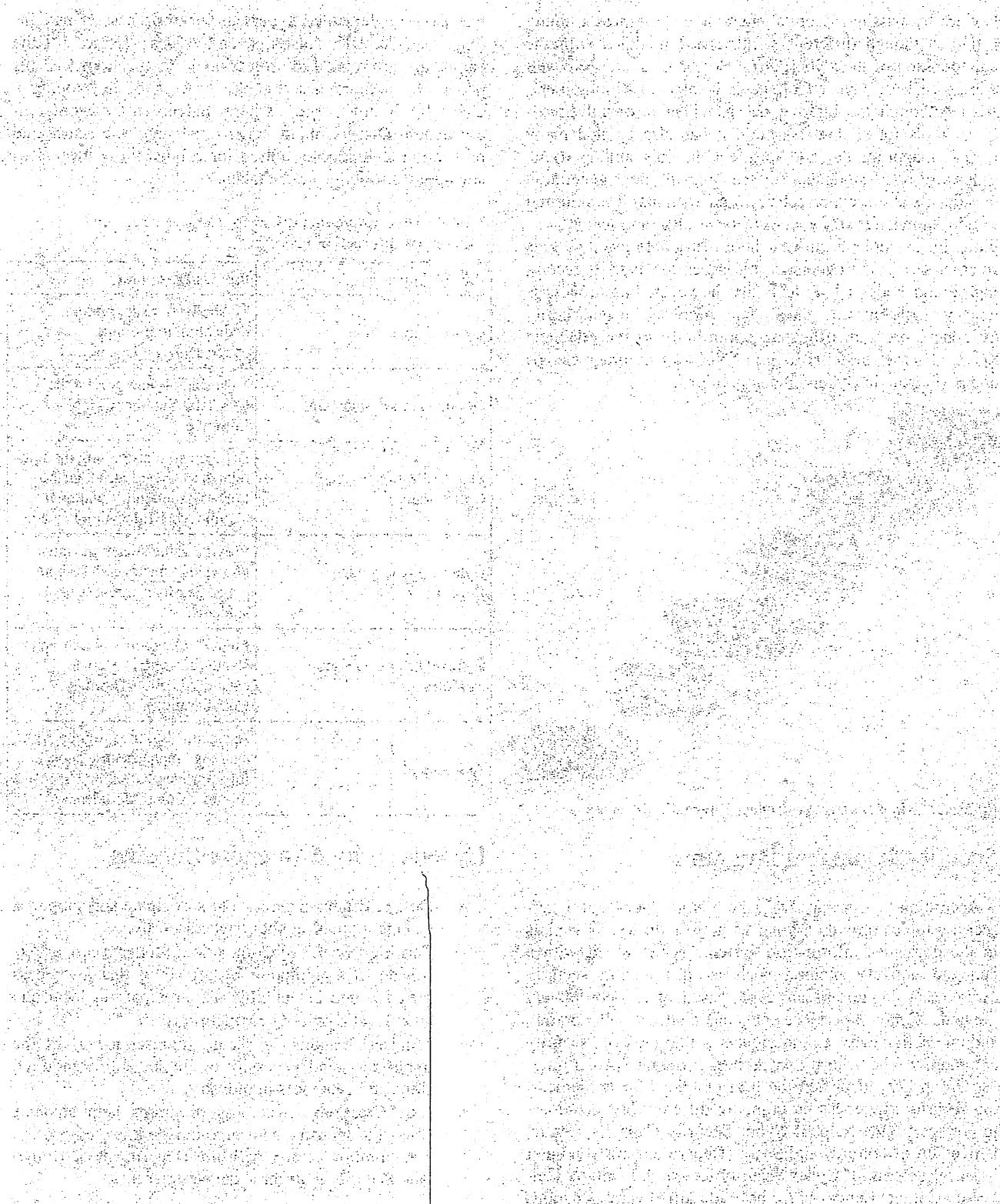
According to Abawajy [21], there is no doubt that cybersecurity topics provide a great value to industry, as well as in the computer information systems (CIS) world with a concrete delivery method such as information security awareness using text-based, game-based, and video-delivery methods. Cyber experiences enhance a strong collaboration and interaction between individuals within the cybersecurity community. The Security Awareness Program Special Interest Group [22] identified the best practices for implementing security awareness programs in different organizations; in contrast, Bada (Global Cyber Security Capacity Centre, University of Oxford) and Sasse (Department of Computer Science, Science of Cyber Security Research Institute, University College London) [23] have identified various nations that have implemented cybersecurity awareness campaigns (e.g., Canada, UK, Australia, and Africa). [Note: All the campaigns are related to professional organizations.] In this paper, the authors describe the process of developing a Cyber-IQ Summer Camp, where students in the Montgomery School District might better understand the issues and prevention techniques required for cybersecurity awareness and applicable actions to be taken.

Table 1. Descriptive Identifiers for the Cybersecurity Awareness Interaction Process

Process Function	Process Descriptor
Cyber Campaign	To show your support and dedication to promote cybersecurity education.
Get Involved Partnership	Visit schools and present the Cyber-IQ Summer Camp Initiative.
Standardization Through Collaboration	Develop similar training modules related to CyberPatriot, an Air Force Association's National Youth Cyber Education Proram.
Cyber-IQ Knowledge Repository	Provide value stream to gain knowledge management about cybersecurity awareness to students.
Cyber-IQ Summer Camp Modules	Four Week modules based on standardization in Step 3 (Standardization Through Collaboration).
Assessment	Assessment of the program with a strong emphasis on feedback for improvement of the Cyber-IQ Summer Camp Modules.

Cybersecurity Awareness Benefits

- Desire: Establish a desire to participate and support a change in mindset about cybersecurity.
- Earn Certificates of Completion: Students earn a Certificate of Completion by attending this awareness program and are eligible to participate in local and state-level Cyber-IQ competitions.
- Mindset: Establish a secure mindset to accept the importance and necessity of implementing required skills and behaviors in industry.
- Jobs Creation: Awareness programs help students enter into industry with prerequisite knowledge (e.g., collaboration efforts with the Department of Homeland Security workforce development).



- Program Assessment: One of the key factors in having a successful effort is being able to prove that your effort is successful. Therefore, different assessment methods will be used, such as surveys on Internet usage attitudes, pre- and post-assessment awareness training data, and identification of the factors that potentially lead to failure/success/modification of the Cyber-IQ Summer Camp program.
- Develop a collaboration with CyberPatriot, an Air Force Association effort to develop standardized modules of training.
- Develop a bridge to encourage students to get certified through standardized security tests and pursue their respective education and certifications in security-related disciplines.

Conclusion

The National Cyber Security Alliance (NCSA) has organized different resources related to Internet literacy, such as cybersecurity that focuses on how to avoid spam and viruses. These free resources can be used in the classroom. Similarly, WiredSafety.org has various free videos and presentations that can be used to develop a secure mindset. To reiterate, the average cost of cybercrime for U.S. retail stores more than doubled from 2013 to an annual average of $7.6 million per company in 2014. Different universities and colleges have engaged K-12 kids in their summer technology programs in order to prepare them for use of technology, but there are no Cyber-IQ Summer Camps (or programs) in the Alabama region, where K-12 students can be educated and informed about the challenges of cybersecurity in today's world. Also, it is crucial for the success of cyber programs that these students be provided with the opportunity to participate in Cyber-IQ competitions.

Acknowledgements

The authors would like to thank the anonymous reviewers for their careful reading of the paper and insightful suggestions for changes, including Amy Smith. This paper is based upon collaboration between Trenholm State Community College Faculty, Faulkner University Faculty, and the Project Manager, Walmart, Inc.

References

[1] The White House, Office of the Press Secretary. (12 February 2013). Remarks by the president in the State of the Union address. Retrieved from https://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address

[2] Computer Security Update. (2011). U.S. Schools not preparing kids for digital age. *Computer Security Update, 12*(6), 1-5.

[3] Butler, K. (2010). Cybersafety in the classroom. *District Administration, 46*(6), 53-57.

[4] eSchool News. (26 February, 2010). Too few schools are teaching cyber safety. Retrieved from http://www.eschoolnews.com/2010/02/26/study-too-few-schools-are-teaching-cyber-safety/

[5] Marcoux, E. (2014). Cyberbullying and technology. *Teacher Librarian, 42*(2), 69-70.

[6] Adele E. H., Indrajit, R., Mark, R., Malgorzata, U., & Zinta, B. (2012). The psychology of security for the home computer user. IEEE Symposium on Security and Privacy. DOI 10.1109/SP.2012.23.

[7] Ponemon Institute. (2014). 2014 global report on the cost of cybercrime. Retrieved from http://www.octree.co.uk/Documents/2014-Global-report-on-the-Cost-of-Cybercrime.pdf

[8] Morgan, S. (2016). One million cybersecurity job openings in 2016. Retrieved from http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#10bc48297d27

[9] Setalvad, A. (2015). Demand to fill cybersecurity jobs booming. Retrieved from http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/

[10] 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), 11-16.

[11] Giannakas, F., Kambourakis, G., Papasalouros, A., & Gritzalis, S. (2016). Security education and awareness for K-6 going mobile. *International Journal of Interactive Mobile Technologies, 10*(2), 41-48.

[12] Air Force Association's CyberPatriot. (2017). The National Youth Cyber Education Program. Retrieved from http://www.uscyberpatriot.org/

[13] Nelson, K. (2015). Cybersecurity jobs are hard to fill. *Washington Examiner*, April 13, 2015. Retrieved from http://www.washingtonexaminer.com/cybersecurity-jobs-are-hard-to-fill/article/2562693

[14] Department of Homeland Security. (2013). Executive Order 13636: Improving Critical Infrastructure Cybersecurity. Retrieved from https://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf

[15] Kortjan, N., von Solms, R., (2014). A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal, 52*, 29-41.

[16] Robles, A.C.M.O. (2012). Cyber portfolio: The innovative menu for 21st century technology. *Psychology Research, 2*(3), 143-150.

[17] Information Security Forum. (2014). From promoting awareness to embedding behaviors: Secure by choice not by chance. [Executive Summary]. Retrieved from https://www.securityforum.org/uploads/2015/12/isf_from-promoting-awareness-to-embedding-behaviours-es1.pdf

[18] Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. National Institute of Standards and Technology (NIST), NIST Special Publication 800-50. Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

[19] Toth, P., & Klein, P. (2014). A role-based model for federal information technology/cyber security training. NIST Special Publication 800-16 Revision 1 (2nd Draft, Version 2). Retrieved from http://csrc.nist.gov/publications/drafts/800-16-rev1/draft_sp800_16_rev1_2nd-draft.pdf

[20] Coventry, D. L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioral insights to improve the public's use of cyber security best practices. Government Office for Science, London, UK. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf

[21] Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behavior & Information Technology, 33*(3), 236-247.

[22] Security Awareness Program Special Interest Group, PCI Security Standards Council. (October, 2015). Best practices for implementing a security awareness program. Retrieved from https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

[23] Bada, M., & Sasse, A. (2014). Cyber security awareness campaigns: Why do they fail to change behaviours? Global Cyber Security Capacity Centre. Retrieved from http://discovery.ucl.ac.uk/1468954/1/Awareness%20CampaignsDraftWorkingPaper.pdf

Biographies

SYED RAZA is an instructor of Computer Information Systems at Trenholm State Community College. He has also finished his Leadership Montgomery training. During his training, he was involved in different community service projects, including the relationship between education and the workforce. He has over 16 years of experience as an educator and software engineer. Dr. Raza may be reached at sraza@trenholmstate.edu

IDONGESIT MKPONG-RUFFIN is a professor and chair of the Computer Science Department at Faulkner University. She received her PhD in computer science and software engineering from Auburn University (2008), a master's degree in computer science from Troy University (2007), an MBA from Tennessee State University (1992), and a bachelor's degree in computer information systems from Freed-Hardeman University (1985). Mkpong-Ruffin has been an educator since 1992. Prior to joining Faulkner's faculty, she was a faculty member in the Computer and Information Science Department at Troy University (2002 – 2004) and ran her own consulting business, IMR Associates, as a software developer and corporate trainer. Her research interests include software security, information assurance, software engineering, data mining, and computer science education. Dr. Idongesit Mkpong-Ruffin may be reached at Imkpong-ruffin@faulkner.edu

SAJID RAZA is currently working as a project manager at Walmart Stores, Inc. Sajid has almost 15 years of IT experience, particularly in the product and service arena. He is an active member of TOASTMASTERS, a non-profit organization, and has served as Vice President, receiving a Competent Communicator (CC) certificate. Moreover, Sajid is a doctoral student at Grand Canyon University in Business Administration. Mr. Raza may be reached at sajid_raza2000@hotmail.com

KEN SCOTT is a senior instructor in Computer Information Systems at Trenholm State Community College, specializing in the field of network engineering, open source systems, and ePortfolio design and development. He holds a doctorate from Auburn University in Educational Leadership and Technology, a master's from Auburn University Montgomery, and a Bachelor of Electrical Engineering from Georgia Southern University. His research interests include ePortfolios, network security, soft skills, and student success factors. He served more than seven years in U.S. Naval intelligence related to physical, digital, and other aspects of national security. Dr. Scott may be reached at kscott@trenholmstate.edu