5-21-2019

Innovations from Academia around Cybersecurity Workforce and Faculty Development

Darrell Norman Burrell
Florida Institute of Technology, dburrell2@thechicagoschool.edu

Innovations from academia around cybersecurity workforce and faculty development

Darrell Norman Burrell
Florida Institute of Technology
dburrell2@thechicagoschool.edu

Abstract

Every year in the U.S., 40,000 jobs for information security analysts go unfilled, and employers are struggling to fill 200,000 other cybersecurity related roles. Colleges and universities have created certificates, undergraduate, and graduate programs to train professionals in these job roles. The challenge to meeting the cybersecurity workforce shortage through degree programs is intensified by the reality of the limited number of cybersecurity experts and faculty at colleges and universities based on the qualifications outlined by regionally accredited and state accrediting bodies. Before 2005 doctoral degrees in cybersecurity did not exist, so many faculty that have been teaching computer science and management information systems that completed their doctoral degree before 2005 could need significant re-education on the academic level in cybersecurity. This paper explores the essential need to develop more doctorate faculty in cybersecurity and to create an 18-credit hour post-doctoral diploma bridge programs in cybersecurity. The conceptual paper uses a review of the literature and previous research to make the argument for these programs.

Keywords: Doctoral studies, cybersecurity doctorates, faculty development, cybersecurity bridge, post doctorate.

Introduction

According to Newman (2016), the cybersecurity threat landscape is continually evolving as malicious cyber actors pursue new vectors to target and capitalize on newly discovered or known vulnerabilities. In 2017 a hacking group known as the Shadow Brokers, claiming to have breached the NSA-linked operation known as the Equation Group. The Shadow Brokers provided samples of the stolen data and attempted to auction off other stolen data (Newman, 2017).

In May of 2017, a strain ransomware virus call WannaCry attacked a series of public and private organizations including temporarily crippling technology-driven operations of several hospitals and medical facilities in the United Kingdom (Newman, 2017). In 2017 there where new revelations about hacking vulnerabilities cell phones, Windows, and the ability to turn some smart TVs into listening devices (Newman, 2017). The top industries targeted by cybercriminals are (1) healthcare, (2) manufacturing, (3) financial services, (4) government, and (5) transportation (Morgan, 2016). These industries are targeted for sensitive information primarily in the healthcare and financial services sectors. Researchers are forecasting the global cost of cybercrime in 2019 to reach over 2 trillion dollars (Morgan, 2016).

The global cybersecurity workforce will have more than 1.5 million unfilled positions by 2020 (Van-Zadelhoff, 2016). Every year in the U.S., 40,000 jobs for information security analysts go unfilled, and employers are struggling to fill 200,000 other cyber-security related roles (Kauflin, 2017). Threats of cyber-attacks have spurred global interest in protecting digital property from external intrusions. The identified risks to American private and public entities were part of an ongoing scenario that placed specific importance on secure, internal, cyber information (Pierce, 2016; Stevenson, 2017). This importance came about because many in the business market had echoed the need for a skilled workforce within cybersecurity, and numerous efforts were made to address those concerns (Pierce, 2016; Stevenson, 2017).

The need for cybersecurity was spearheaded by the rise in cybercrime (Pierce, 2016; Stevenson, 2017). Newman (2017) described cybercrime as the use of communication and information technologies to carry on illegal activity. Cybercrime activity was conducted with the utilization of devices including television, cellular phones, radios, computers, networks, or communication application (Newman, 2017). Newman (2017) noted that cybercrime was widespread and was not limited to petty. Morgan (2016) and Newman (2017) indicated that cyber-attacks and malicious hackers have increased with multiple large corporations becoming victims of data breaches. Morgan (2016) noted firms were growing more dependent on cyber connectivity to remain relevant in an increasingly global market, and this has left many of them vulnerable. American organizations made changes to their IT infrastructure to deflect the onset of external threats from cybercriminals as they continued to grow (Van- Zadelhoff, 2016). Newman (2017) identified the cyber-attacks came from multiple sources with a variety of agendas. Newman (2017) noted the cyber threats were distinguished by intent and motivation of the attacker.

The review of the literature

The onslaught of cyber-attacks enhanced the need to fill positions focused on the prevention of data breaches (Pierce, 2016; Stevenson, 2017). Besides, the shortage of skilled personnel provided a new dynamic to finding qualified workers that understood the complexities of cybersecurity, and that could contribute significantly to the overall needs of the company (Pierce, 2016; Stevenson, 2017).

Information technology related positions required consistent training to remain on top of constant changes in the field (Andre 2016). With a good understanding of the threats that a professional cybersecurity face, the academic community was the first to attempt to fill the gap in knowledge for practitioners (Van-Zadelhoff, 2016). The field of computing before 1990 was very straightforward (Force, 2001). The 1968 Association for Computing Machinery (ACM) report was the first of its kind to describe the guidelines of computing (Force, 2001). The 1978 ACM report provided details on course descriptions with specific bibliographic references (Force, 2001). In 1983, IEEECS and the Association for Computing Machinery jointly published a more in-depth course description of specific topic areas for both computer science and engineering (Tucker et al., 1991).

The events of September 11, 2001 created new areas of focus including homeland security and cybersecurity. The ACM acknowledges that the scope of what is called computing has drastically changed as of the filing of the 2001 ACM report (Curricula, 2001). Information systems had to address many new challenges with the growth of computing power. Information technology programs began to appear (Force, 2001). Besides, security and cryptography are explicitly listed as reasons why the curriculum of the computing field needed revision (Force, 2001).

The 2004 ACM identifies the differences and similarities of the five major computing disciplines (Shackelford et al., 2006). The options were computer science, electrical engineering, or information systems. The focus of computer science is on programming software, and electrical engineering is on hardware. The focus of information systems is on using hardware and software to meet organizational goals (Shackelford et al., 2006). The only change before 1990 in the computing field was the introduction of computer engineering, which was a specialization of electrical engineering due to the opening of the microprocessors (Shackelford et al., 2006). In 2005, an ACM report identified dramatic growth has been seen in some computing disciplines (Shackelford et al., 2006).

A hindrance to growth in the cybersecurity field is clearly defined paths of professional development. Experience and training seem not to be a typical discussion within the cybersecurity community. Most professionals who attend training or obtain experience do so by job-hopping or by attending training at the expense of the cybersecurity professional (Li & Daugherty, 2015). Others seek academic degrees in cybersecurity and information security. As such, it is easy to see with the shortages of professionals in both the entry and higher complexity roles that the burden falls on the existing cybersecurity professionals to develop the needed skills (Andre, 2016).

An additional hindrance to the developing more professionals falls on universities that do not offer programs in cybersecurity that can re-train older workers interested in career changes and can develop new ones. One factor that increases the number of older workers in the workforce is the improvement in health care and resultant life expectancy (Cappelli & Novelli, 2010). Therefore, leveraging the experience of older workers is of vital importance to engage and help develop the existing workforce (Cappelli & Novelli, 2010). Currently, a large percentage of knowledge is lost due to the unrealized value of this portion of the workforce.

According to the President's Council of Advisors on Science and Technology (PCAST) (2012), the US faces a shortage of a million Science, Technology, Engineering, and Mathematics (STEM) professionals more than those currently being developed. It will require a 34% increase in the development of science and technology professionals each year (PCAST, 2012). To make things worse, there is a leaky development pipeline meaning that less than 40% of students who start college interested in technology fields graduate (Strayhorn, 2010). “Increasing the retention of STEM majors from 40% to 50% would, alone, generate three-quarters of the targeted one million additional STEM graduates over the next decade” (President's Council, 2012). STEM degree completion rates indicate improvement over the past decade; however, there are still significant gaps among women and minorities (Strayhorn, 2010).

According to Palmer, Maramba, and Gasman (2013), U.S. institutions need to improve the teaching and retention approaches for those in technology related academic programs. Meeting the workforce demand through educational offerings becomes more challenging when large sectors the population that include women and peoples of color are significantly underrepresented in these academic fields and academic programs (Burrell & Nobles, 2018).

Several universities have created successful approaches and pathways that are working (Burrell & Nobles, 2018). During what is a national crisis in STEM and especially cybersecurity, some institutions are outperforming others. According to Palmer, Maramba, and Gasman (2013) historically black colleges and universities (HBCUs) produce the most significant number of underrepresented minorities completing STEM bachelor's degrees, which has the potential to create a viable pipeline for cybersecurity professionals, which is a frequently overlooked natural resource for the country's economy. Women currently comprise approximately half of the United States' workforce, and it is forecasted that underrepresented minorities will constitute 32% of the population of the U.S. in 2020 with Hispanics expected to be 25% of the population by 2050 (Herling, 2011). These groups represent potential cybersecurity employees and likely future cybersecurity faculty that can be instrumental in developing the next generation of cybersecurity professionals at colleges in universities.

Organizations need to strive to improve their strategy and practices to make use of the experience and knowledge that exists with their experienced workers (Cappelli & Novelli, 2010).
These hindrances contribute to the obstacles the cybersecurity professional organization or education provider must address to increase the number of professionals and reduce the skill gap that exists currently (Andre, 2016).

These hindrances also highlight the importance of understanding the complexities of the issue and the need to find both academic and professional solutions to develop more professionals with critical knowledge and expertise in cybersecurity (Andre, 2016). The current shortage of cybersecurity practitioners requires an active approach to resolving the problem both in the near and long term (Andre, 2016). While colleges and universities are offering more cybersecurity degree options, they still have a shortage of qualified faculty that can teach in these programs. Meeting workforce shortage needs of business requires universities to meet the workforce shortage needs of universities of qualified faculty that can teach in these programs especially those that are female and from backgrounds that have historically been ignored or underrepresented (Delia 2015). According to Burrell and Nobles (2018) the solution requires innovative thinking and new approaches including the establishment of strategic collaborations between education, corporations, the federal government, and professional associations to not only train cybersecurity professionals, but fund graduate and doctoral study for professionals that are interested in faculty jobs which can educate and train those interested in academic programs in cybersecurity.

The development of non-traditional Doctoral Programs

Several accredited US universities have had success developing non-traditional doctoral programs that offer limited face to face teaching residencies and online learning. These programs allow students from all over the world to complete a doctoral degree in information security or cybersecurity while working full time. These are all brick and mortar universities that are leveraging their campus resources to engage professionals with significant work experience in the field, which with a doctorate degree, could become effective faculty members in the future. These programs have several similar characteristics like either online or limited residency offerings and cohort formats. These schools include:

1. The University of Cumberlands in Williamsburg, Kentucky, the USA that has an online Ph.D. in Information Technology with the ability to study cybersecurity and blockchain technologies.

2. Marymount University in Arlington, VA, USA has an online and face to face Doctor of Science in Cybersecurity.

3. Dakota State University in Madison, South Dakota, USA has an online Ph.D. in Information Security.

4. Capitol Technology University, in Laurel Maryland, USA has a hybrid/executive DSc in Cybersecurity and a Ph.D. in Decision and Data Sciences.

5. Colorado Technical University, in Denver, Colorado, USA has a hybrid/executive Doctor of Science (DSc) - Cybersecurity and Information Assurance

6. Pace University in Westchester, NY has an online Doctor of Professional Studies (DPS) in Computing

These universities with flexible doctoral programs geared towards working professionals and executives in the cybersecurity fields could be the perfect organizations to develop and launch this post-doctoral cybersecurity diploma that can be a bridge program for those interested in becoming cybersecurity faculty. These programs thought innovative often produce graduates that find challenges with integration and acceptance as faculty members in research-intensive universities because these programs are not offered in traditional on-campus Ph.D. program formats. Maybe one answer could be traditional universities providing" post-doctoral fellowship to faculty hire programs" where faculty from non-traditional doctoral programs can be immersed in the culture, expectations, funded research methods, and the publishing processes that are the norm at research universities. These fellowships could allow universities with a critical need for cybersecurity faculty to collaborate with graduates from non-traditional doctoral programs.

The need and value of a Post-Doctoral Bridge Program

The higher education response to workforce shortages of cybersecurity professionals has been the development of certificate, associates, bachelor's, and graduate degrees. The challenge of meeting the cybersecurity workforce shortage through degree programs is intensified by the reality of the limited number of cybersecurity experts and faculty at colleges and universities (McClurg, 2015). Before 2005 doctoral degrees in Cybersecurity did not exist, so many faculty that have been teaching computer science and management information systems need significant re-education. Those that are highly experienced in cybersecurity fields that have doctorates in disciplines like business and education could also be prime candidates advanced level cybersecurity education. A significant solution to address this issue in several areas if the creation of "Cybersecurity Post-Doctoral Diploma" which essentially would be an 18-credit hour post-doctoral program with 6 classes and capstone research experience of academic publication that would provide new education to faculty with doctorate degrees in Computer Science, Management Information Systems, Technology Management, Educational Technology as well as those with significant work experience and certifications in cybersecurity but may have a doctorate in another discipline . This kind of program could be developed to produce more cybersecurity faculty that could help meet the demands for new degree programs and the workforce demands of industry. For those universities that do not have faculty with expertise, these courses could be taught by adjunct faculty or contracted faculty with cyber expertise from other universities, with the goal in mind of building campus expertise and bench strength in cybersecurity instruction for those that do not have the knowledge. This program could be offered in a cohort/executive format where 15-20 participants could complete the program in an online or hybrid manner as a collective group in 9 months. Universities could even offer funding for a future service/teaching agree with the university providing the funding, meaning that for each course funded the program graduate would have to teach two classes at the university as a service commitment. The result is the creation of an innovative strategy to develop faculty that can teach cybersecurity at universities that are committed to meeting the enormous workforce demand.

References

1. Andre, P. (2016). A phenomenological study of frontline hiring professionals that recruit in a cybersecurity world (Order No. 10250990). Available from ProQuest Dissertations & Theses Global. (1868414289). Retrieved from https://search-proquest-com.contentproxy.phoenix.edu/docview/1868414289?accountid=35812

2. Burrell, D., Nobles, C. (2018). Recommendations to Develop and Hire More Highly Qualified Women and Minority Cybersecurity Professionals. Proceedings of ICCWS 2018 13th International Conference on Cyber Warfare and Security. Academic Conferences International Limited.
3. Cappelli, P. (2008). Talent management for the twenty-first century. Harvard business review, 86(3), 74.
4. Cappelli, P., & Novelli, W. D. (2010). Managing the Older Worker: How to Prepare for the New Organizational Order. Harvard Business Press.
5. Clancy, M. (2012). Improving faculty professional development in higher education high-tech programs: An action science research study of self-directed professional development (Order No. 3542028). Available from ProQuest Dissertations & Theses Global. (1143242820). Retrieved from https://search-proquest-com.contentproxy.phoenix.edu/docview/1143242820?accountid=35812

6. Curricula, C. (2001). Computer Science. IEEE CS, ACM Joint Task Force on Computing Curricula.
7. Delia, C. (2015). Exploring the social and organizational factors of the shortage of women in information technology: A multiple case study (Order No. 3732277). Available from ProQuest Dissertations & Theses Global. (1746623174). Retrieved from https://search-proquest-com.contentproxy.phoenix.edu/docview/1746623174?accountid=35812
8. Force, J. T. (2001). Computing curricula 2001: Computer science. Retrieved from https://www.acm.org/education/curric_vols/cc2001.pdf
9. Fuller, C. R. (2016). Shortening the skills gap: An exploratory study of cybersecurity professional experience (Order No. 10250901). Available from ProQuest Dissertations & Theses Global. (1868417653). Retrieved from https://search-proquest-com.contentproxy.phoenix.edu/docview/1868417653?accountid=35812
10. Herling, L. (2011). Hispanic women overcoming deterrents to computer science: A phenomenological study (Order No. 3505844). Available from ProQuest Dissertations & Theses Global. (1013441827).
11. Kauflin, J. (2017, March 16) The Fast-Growing Job with A Huge Skills Gap: Cyber Security. Forbes
12. Li, J., & Daugherty, L. (2015). Training cyber warriors: What can be learned from defense language training? Santa Monica, CA: RAND National Defense Research Institute.
13. McClurg, J. D. (2015). Cybersecurity in higher education: Oversight and due diligence (Order No. 10291072). Available from ProQuest Dissertations & Theses Global. (1846958719). Retrieved from https://search-proquest-com.contentproxy.phoenix.edu/docview/1846958719?accountid=35812
14. Morgan, S. (2016, May 13). Top 5 industries at risk of cyber-attacks. Forbes.com. Retrieved on February 17, 2018, from https://www.forbes.com/sites/stevemorgan/2016/05/13/list-of-the-5-most-cyber-attacked-industries/#1edfc762715e
15. Newman, L. (2017, July 1) The biggest cybersecurity disasters of 2017 so far. WIRED.
16. Palmer, R. T., Maramba, D. C., & Gasman, M. (Eds.). (2013). Fostering Success of Ethnic and Racial Minorities in STEM: The Role of Minority Serving Institutions. New York, NY: Routledge. 264 pp.
17. Pierce, A. O. (2016). Exploring the cybersecurity hiring gap (Order No. 10250186). Available from ProQuest Dissertations & Theses Global. (1848667353). Retrieved from https://search-proquest-com.contentproxy.phoenix.edu/docview/1848667353?accountid=35812
18. President's Council of Advisors on Science and Technology. (2012). Report to the president: Engage to excel: Producing one million additional college graduates with degrees in science, technology, engineering, and mathematics. Retrieved from http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-engageto-excel-final_2-25-12.pdf
19. Strayhorn, T. L. (2010). Undergraduate research participation and STEM graduate degree aspirations among students of color. New Directions for Institutional Research, 2010 (148).
20. Sweem, S. L. (2009). Leveraging employee engagement through a talent management strategy: Optimizing human capital through human resources and organization development strategy in a field study (Order No. 3349408). Available from ProQuest Dissertations & Theses Global. (305162419). Retrieved from https://search-proquest-com.contentproxy.phoenix.edu/docview/305162419?accountid=3581
21. Shackelford, R., Lunt, B., McGettrick, A., Sloan, R., Topi, H., Davies, G., Lunt, B. (2006). Computing curricula 2005: The overview report. [Association for Computing Machinery] ACM [Special Interest Group on Computer Science Education] SIGCSE, 38(1), 456-457.
22. Stevenson, G. V. (2017). *Cybersecurity implications for industry, academia, and parents: A qualitative case study in NSF STEM education* (Order No. 10624075). Available from ProQuest

Dissertations & Theses Global. (1958945736). Retrieved from https://search-proquest-com.contentproxy.phoenix.edu/docview/1958945736?accountid=3581

23. Tucker, A. B., Aiken, R. M., Barker, K., Bruce, K. B., & Cain, J. T. (1991). Computing curricula 1991: Report of the ACM/IEEE-CS Joint Curriculum Task Force. New York, NY: Association for Computing Machinery Press/IEEE Press.
24. Van- Zadelhoff, Marc (2016, September). The Biggest Cybersecurity Threats Are Inside Your Company. Harvard Business Review.
25. Wilson, M. D. (2015). A qualitative case study of the talent management process across project-oriented companies within the intellect industry (Order No. 3687744). Available from ProQuest Dissertations & Theses Global. (1669973498). Retrieved from https://search-proquest-com.contentproxy.phoenix.edu/docview/1669973498?accountid=35812