RE-ENGINEERING THE CYBERSECURITY HUMAN CAPITAL CRISIS

Morgan Zantua, Marc Dupuis, Barbara Endicott-Popovsky

University of Washington Tacoma

Abstract

The demand for cybersecurity professionals continues to significantly outpace the supply with a projected worldwide shortage of two million by 2017. At the same time, there are large numbers of transitioning military personnel that have important technical skills that could be coalesced into addressing this demand. This paper examines the development and proposed deployment of a project to do just this: Cybersecurity Rapid Education Apprenticeship Training to Employment System (CREATES). Challenges and benefits are discussed.

Keywords: transitioning military personnel, cybersecurity supply and demand, veterans, training

Introduction

While our nation's infrastructure is vulnerable to cyber-attack and cyber misuse, there is a critical deficit of cybersecurity professionals to address the problem (Burley, Eisenberg, & Goodman, 2014). Thousands of career positions in information assurance and cybersecurity are going unfilled (Conklin, Cline, & Roosa, 2014; Cranor L.F. & Sadeh N., 2013). Yet, the demand is only going to continue to increase to unprecedented levels. A report by the United Kingdom's House of Lords indicates a worldwide shortage of two million cybersecurity professionals by 2017 (Oltsik, 2014).

At the same time the military drawdown is releasing personnel with intensive technical training, often in the computing sciences (Mitcham, 2013; Soldan, Schulz, Gruenbacher, Vogt, & Natarajan, 2011). These veterans could leverage their background with appropriate academic education in information assurance (IA) and cybersecurity to fill the country's need for IA professionals.

This paper briefly explains the background of the problem, an approach to address the problem, and how this approach can later be refined and disseminated to other interested entities for maximum impact. Ultimately, the goal is to leverage our transitioning military personnel to address the severe shortage of cybersecurity professionals. This approach will serve as a win-win-win with direct benefits for veterans, public organizations, and the private sector.

Background

The Center for Information Assurance Cybersecurity (CIAC), housed at the Provost's office at the University of Washington and encompassing the University of Hawaii, is an incubator for cutting edge research in Information Assurance (IA) curricula development. Since 2007, Endicott-Popovsky and Popovsky's initial research has developed:

- 107 students earning a certificate in IA
- 40 Masters of Science in Info. Management students with a concentration in IA
- 4 Masters of Library and Information Science students with a concentration in IA
- 76 students receiving a Master of Strategic Planning in Critical Infrastructure
- 26 Master's in Cybersecurity and Leadership
- 8 PhD students across all disciplines, with an IA focus

In 2012, Dr. Endicott-Popovsky's Information Security Risk Management (ISRM) curriculum was offered on Coursera. Over 50,000 students globally enrolled in the free ISRM 10-week course.

Based on the track record of the CIAC, it was awarded a two-year grant called VetsEngr in 2010 (NSF award EEC-1037814). The purpose of the grant was to conduct case studies of returning veterans to determine the feasibility of transitioning these individuals into cybersecurity roles through appropriate education in information assurance. As a result of this initial study, NIST recently awarded a one-year bridge grant to lay the foundation of a model within Washington State to guide National Guard, Reservists, and transitioning military into public two- and four-year cybersecurity-related programs.

The model, Cybersecurity Rapid Education Apprenticeship Training to Employment System (CREATES), builds a pipeline, with on and off ramps, throughout the network of two-year associate degrees, four-year college and university degrees, certificates, masters, and doctoral degrees. In the first phase of the grant a database will provide a complete guide to education resources within Washington State. A companion guide to over 180 NIETP Centers of Academic Excellence and Research in Information Assurance will be made available to military transitioning out of Washington.

The question becomes how to identify those most suited to this profession. The initial pilot participants were highly selected volunteers initially interested in a digital forensics class. Candidates were interviewed, assessed to determine background in computer technology, and culled through to determine verbal and mathematical aptitudes. This resource intensive process relied heavily upon candidates knowing enough about Cybersecurity/Information Assurance to have an interest in Digital Forensics.

Could a broader range of individuals do equally well? And how can the candidates most likely to succeed be identified? If we want to increase the numbers we serve, and we certainly need to, then we must develop an efficient process to identify candidates with “the right stuff” to succeed in the ubiquitous and interdisciplinary cybersecurity field.

The Problem

The Department of Labor, Bureau of Labor Statistics reports a 37% increase in security analysts since 2012 and projects continued demand for individuals with this skill set (Bureau of Labor Statistics, 2014). Amazon, Microsoft, and other major companies pay top dollar for American talent and continue to import talent from around the globe to supplement their cybersecurity workforce (Fourie et al., 2014). Government agencies (city, county, state and federal) have the same gaps in filling their workforce needs (Paulsen C., McDuffie E., Newhouse W., & Toth P., 2012).

This study will link the demand side of the burgeoning cybersecurity workforce with the supply side coming from the transitioning military community. The supply side for cybersecurity professionals has been a major impediment to addressing the shortage and this is one way to bridge that gap (Wilson & Ali, 2011). Additionally, one major economic challenge facing the Department of Defense is the high cost of unemployment benefits being paid out to transitioning service members (Kleykamp, 2013). This project will help address this economic challenge as well.

Imagine a proactive methodology used to identify high potential cybersecurity professionals early in the military transition process. Regardless of the Army’s Military Occupational Status, Air Force Specialty Code, or the Navy’s rating, talent can be identified and moved into the CREATES pipeline in anticipation of transitioning out of the military and into government or private sector cybersecurity careers.

Challenges, Benefits, and Proposed Approach

Conducting this research with the military provides both short- and long-term benefits. The military represents a diverse population for this study, especially with respect to ethnic diversity (Lundquist, 2008). And as discussed earlier and studied in the VetsEngr grant, today’s military receive state-of-the-art technical training; yet few move forward utilizing their GI Bill to leverage this experience into academic pathways enabling them access to higher paying cybersecurity positions in government and industry.

Likewise, those that do utilize their GI Bill often choose community colleges or for-profit colleges rather than universities, such as state or private not-for-profit universities (Field, Hebel, & Smallwood, 2008). This is due primarily to the convenience provided by community colleges and for-profit entities, as well as the greater likelihood that transitioning military personnel will receive credit for training they received while on active duty. In the process, students may be limiting their options and eventual career opportunities, such as cybersecurity.

This research will examine a broader base of individuals for cybersecurity careers and will incorporate frameworks based on complementary efforts from entities such as NIST (Paulsen C. et al., 2012). The initiative will generate awareness and move more individuals into the CREATES pipeline. The assessment tool will be ‘beta tested’ on transitioning military and reserve components. As the tool is refined, it can be utilized on a larger pool of candidates and help them to enter the cybersecurity field to address the shortage of cybersecurity professionals in the workforce. A longitudinal study will examine the long-term impact of assessment upon the military transitioning: their career choice within cybersecurity, wage progression, and professional development.

Conclusion

Developing an accessible assessment tool and replicating the CREATES model will do more than address the initial shortage of cybersecurity professionals. For example, it will be able to help combat the lack of female representation in the cybersecurity field, which has been a significant issue resulting in a deficit of diversity in viewpoints (Dampier, Kelly, & Carr, 2012).

Additionally, the tool will be a resource provided to several different entities. For example, the CIAC proposes to introduce the assessment tool to academic organizations and K-12 systems throughout the CIAC network of NIETP Academic Centers of Excellence and professional organizations such as IEEE, University Professional Continuing Educator Association (UPCEA), Cyberwatch, Colloquium Information Security Systems Education (CISSE), NIST, and the Council of College and Military Educators (CMEC).

On October 4, 1957 Sputnik changed the course of American education for the next two decades and subsequently built a strong technical workforce that kept America at the forefront of the space race and technological innovation (Wissehr, Concannon, & Barrow, 2011).

September 11th, this generation’s wake-up call, brought a renewed patriotism to many who chose to protect and defend their country (Poulin, Silver, Gil-Rivas, Holman, & McIntosh, 2009; Sahar, 2008). Development and utilization of this assessment tool and the instantiation of CREATES provides an opportunity to harness the talent and patriotism of this generation to proactively protect and defend our nation against an impending Cyber 9/11.

References

Bureau of Labor Statistics. (2014). *Information Security Analysts*. U.S. Department of Labor. Retrieved from http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Burley, D. L., Eisenberg, J., & Goodman, S. E. (2014). Would cybersecurity professionalization help address the cybersecurity crisis? *Commun. ACM*, *57*(2), 24–27.

Conklin, W. A., Cline, R. E., & Roosa, T. (2014). Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors. *System Sciences (HICSS), 2014 47th Hawaii International Conference on*, 2006–2014. doi:10.1109/HICSS.2014.254

Cranor L.F., & Sadeh N. (2013). A shortage of privacy engineers. *IEEE Secur. Privacy IEEE Security and Privacy*, *11*(2), 77–79.

Dampier, D., Kelly, K., & Carr, K. (2012). Increasing Participation of Women in Cyber Security. In *ASEE-SE Regional Conference, Starkville, MS*.

Field, K., Hebel, S., & Smallwood, S. (2008). Cost, convenience drive veterans' college choices. *Chronicle of Higher Education*, *54*(46), A1–A14.

Fourie, L., Pang, S., Kingston, T., Hettema, H., Watters, P., & Sarrafzadeh, H. (2014). The global cyber security workforce: an ongoing human capital crisis. *Global Business and Technology Association*.

Kleykamp, M. (2013). Unemployment, earnings and enrollment among post 9/11 veterans. *Social Science Research*, *42*(3), 836–851. doi:10.1016/j.ssresearch.2012.12.017

Lundquist, J. H. (2008). Ethnic and Gender Satisfaction in the Military: The Effect of a Meritocratic Institution. *American Sociological Review*, *73*(3), 477–496.

Mitcham, M. (2013). Academic Recognition of Military Experience in STEM Education. *American Council on Education*.

Oltsik, J. (2014, December 9). Cybersecurity Skills Shortage Panic in 2015? Retrieved from http://www.networkworld.com/article/2857305/cisco-subnet/cybersecurity-skills-shortage-panic-in-2015.html

Paulsen C., McDuffie E., Newhouse W., & Toth P. (2012). NICE: Creating a cybersecurity workforce and aware public. *IEEE Secur. Privacy IEEE Security and Privacy*, *10*(3), 76–79.

Poulin, M. J., Silver, R. C., Gil-Rivas, V., Holman, E. A., & McIntosh, D. N. (2009). Finding social benefits after a collective trauma: Perceiving societal changes and well-being following 9/11. *Journal of Traumatic Stress*, *22*(2), 81–90. doi:10.1002/jts.20391

Sahar, G. (2008). Patriotism, Attributions for the 9/11 Attacks, and Support for War: Then and Now. *Basic and Applied Social Psychology*, *30*(3), 189–197. doi:10.1080/01973530802374956

Soldan, D. L., Schulz, N. N., Gruenbacher, D. M., Vogt, B. M., & Natarajan, R. (2011). Work in progress — Streamlining pathways to engineering degrees for military veterans. *Frontiers in Education Conference (FIE), 2011*, F3J–1. doi:10.1109/FIE.2011.6142736

Wilson, A., & Ali, A. (2011). The Biggest Threat to the U.S. Digital Infrastructure: The Cyber Security Workforce Supply Chain. *Academy for Studies in Business*, *3*(2), 15.

Wissehr, C., Concannon, J., & Barrow, L. H. (2011). Looking Back at the Sputnik Era and Its Impact on Science Education. *School Science & Mathematics*, *111*(7), 368–375.