Open Access License Notice

Cybersecurity Career Profiling

Morgan Andreanna Zantua, M.A.
UW CIAC Director of Workforce Development

Barbara Endicott-Popovsky, Ph.D.
Ph.D. Executive Director UW CIAC

Abstract - Professionalization of a cybersecurity workforce is under development from multiple perspectives. Government agencies, the military and academic institutions strive to standardize excellent curriculum and career pathways, certifications, job descriptions classifications are contributing to the effort. In its infancy is the development of statistically validated psychological profiles of candidates' possessing the talent, disposition and interest to excel in the rapidly maturing field and diversifying field of cybersecurity. To address this gap, we propose to borrow from the well- established medical profession and utilize psychological profiling protocols tailoring a statistically validated career assessment tool to build cybersecurity psychological profiles of two markedly different cybersecurity career pathways. Once profiles are defined and validated we propose several Next Steps. Team members and industry partners comparing the psychological profiles can advise or refute a case to conduct additional profiling of additional cybersecurity career pathways. The assessment protocols and methodology will be disseminated to multiple communities at regional, national and international conferences to increase the diversity and numbers of talent entering the cybersecurity career pipeline.

1 INTRODUCTION

Talent demands discussed in the Human Capital Crisis in Cybersecurity in 2010 (Evans, 2010) are dwarfed by current projections for cybersecurity professionals. "The demand for these skilled workers is increasing enrollments in programs, but the demand will continue to grow as business computing increasingly moves toward the cloud." (Suciu, 2015). Jobs in cybersecurity grew 74% from 2007 to 2013

(Burning Glass Technologies, 2015) more than twice the growth rate of all IT jobs. While IT has been considered the entryway into cybersecurity, positions there are growing realization that the cybersecurity workforce shortage cannot rely on current IT programs or the existing IT workforce to meet the growing demand. As cybersecurity matures as an interdisciplinary profession, additional capabilities and knowledge beyond IT skills are required to perform and excel.

Initiatives to professionalize cybersecurity is underway. Research by Dr. Diana Burley, George Washington University Professor and Chair of Institute for Information Infrastructure Protection, compliments (Burley, 2014) extensive work by National Institute Education Training Programs (NIETP) to develop 2Y and 4Y+ educational program integrating Knowledge Units into curriculum while National Institute Cybersecurity Education (NICE) released for comment the NICE Cybersecurity Workforce Framework (NCWF) (Newhouse, 2016). Digitization's innovation impact private sector's workforce needs (Pental, 2017) with new security roles challenging the extensive task list presented in NCWF. The Department of Homeland Security's Cybersecurity Workforce Development Toolkit walks readers through a systemic approach to maturing their organization's cybersecurity workforce culture. (US Department of Homeland Security, 2016)

These major initiatives focus on the supply side of training and educating cybersecurity talent and the demand side of identifying career pathways, job descriptions and tasks performed by people working in cybersecurity jobs. However, to fully re-engineer the human capital crisis in cyber security, assessment tools are required to identify talent from multiple sources with the propensity to succeed in rapidly developing cyber security career pathways. The propensity to succeed describes candidates able to excel in learning acknowledged cybersecurity knowledge units and possess the psychological profile, temperament and interest, to thrive in the differentiated areas of cybersecurity. To meet the projected demands for a well-trained, competent cybersecurity workforce, identifying and nurturing cybersecurity talent nationally and providing career guidance to individuals within

our country's borders is of the highest priority to meet the increasing need of high-quality cyber security professionals across multiple industries and economic sectors.

2 PREVIOUS WORK

Current challenges include identifying individuals with the combination of career training potential, and psychological profile to work in cyber security. Industry professionals acknowledge it takes more than 180 days to fill positions and 64% of applicants aren't qualified to perform required job functions. (ISACA, 2017) This industry survey mirrors conversations with leading academic researchers and a Chief Information Officer from a national laboratory; all commented on the need for more than people who just follow the check list. The demand is growing for critical thinkers who are adept at delivering cybersecurity to decision makers with diverse technical and non-technical backgrounds.

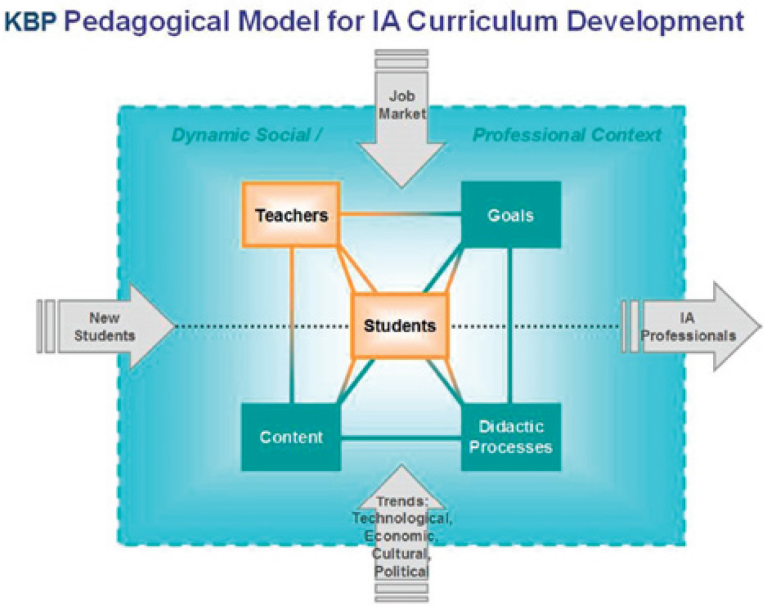
University of Maryland researchers and the Air Force are wrestling with similar issues. (Johnson, 2015) Initiatives to professionalize cybersecurity, meet the growing demand to fill the pipeline with more people, identify talent to guide individuals into the career pathway best suited to the psychological profile and contribute to the demand for this project.

The research team proposes to use a recent research study from the medical profession, a field professionalized 169 years ago to address this problem. Within the medical field, surgical specialties are highly competitive and lucrative professions. A research project to define a psychological profile for Surgical Burn Unit residents provides a lesson and protocol for selecting talent into cybersecurity.

In 2010 a team of psychologists published the "Psychological Profile of Surgeons and Surgical Residents (Foster, 2010) Twenty percent of surgical residents were not completing their residency at the Maricopa Burn Unit. This proved expensive to the surgical resident and exorbitant to the hospital. Hospital administration calculated the cost of $1,000,000 per failed resident. An Arizona State University research team developed a psychological profile overlaid on a performance curve developed from the pool of Attending Surgeons and Surgical Residents. Using

approved Institutional Review Board standards, the World of Work Inventory (WOWI) was administered and the anonymized data utilized to build a psychological profile of high performing Attending Surgeons and Surgical Residents. The Surgical Psychological profile, built a profile to reflect the psychological profile of high performing surgeons suited to work in a Burn Unit. Since WOWI has been included and heeded during the selection process of Surgical Residents, the attrition rate dropped significantly, sparing residents from reapplying to different surgical programs, saving the hospital millions of dollars, increasing surgeon retention and improving patient satisfaction with medical treatment.

In recent decades medicine, as a mature profession, acknowledged psychological patterns connected to specializations (Reich, 1999) are defined. Cybersecurity proceeds towards professionalization and increasingly diverse career pathways are emerging. Intertwined with interdisciplinary implications requiring diverse skill sets and varied experiential backgrounds, the potential for varied psychological patterns and talent profiles are surfacing. (Pental, 2017)



For the past fourteen years, researchers at the University of Washington using the KBP Pedagogical Model for IA Curriculum Development (Endicott-Popovsky, March 2014) have successfully transitioned 679 predominantly mid-career IT professionals into Information Assurance positions. The student centric KBG model accelerates the learning capabilities of students transitioning into cybersecurity and increases the supply of IA professionals by tapping into the stream of mid-career IT workers. In the early stages of research cycle outreach to non-IT professionals, transitioning military and non-traditional workers began. In 2010 researchers received multiple NSF grants. The Scholarship for Service grant supported the development of 17 cyber corps members to study cloud security and critical infrastructure. The second grant was based on VETS ENG GI Bill utilization to study transitioning Active Duty and National Guard service members to identify why more service members were not entering STEM (specifically cybersecurity) disciplines. (National Science Foundation, April 2009) During this study, university researchers interfaced with a team of workforce development professionals, transition specialists hired to provide career guidance and employment transition services to returning service members. Between 2009 to 2013, over 1,000 members of the military, Reserve, Guard and Active Duty received the same assessment tool used to profile surgical residents in the Maricopa Burn Unit study. For the purposes of the VETS ENG study, members received assessment, career coaching. During the year a cohort of 10 soldiers completed a graduate certificate in Information Assurance and Risk Management. Ninety percent of the study group obtained employment, additional certifications or degrees, including the cyber security related master degrees in Infrastructure Planning and Management, Information Management Systems and Cybersecurity and Leadership.

The university researchers collaborated with the workforce development transition coach incorporating additional career guidance, professional coaching coupled up with the student focused life-long learning methodology promoted as part of the Center for Academic Excellence's philosophy." Become a Professional" and 'finding your swim lane' within the cyber security career pathways allowing

students to complete a WOWI and receive a coaching session based upon their customized profile. Feedback report in hand, students evaluate the career pathways and select areas of interest based in the NIST/NICE workforce framework matched to their career profile and interests. Their next step identifies gaps in their knowledge, certifications or education, as they personalize their cybersecurity tool kit. Students develop actionable strategies to close these gaps to make themselves competent, competitive and marketable for their targeted career specialty.

In response to the diversification of career pathways researcher and career coach proactively developed and included a specific career guidance and coaching module at the beginning of the first quarter in the three-quarter certificate. This module prepares all students, military, non-military, IT professionals and 'outliers' with a customized profile and an understanding of the emerging career pathways within cybersecurity. This clarity enables them to build a professional network from guest lecturers, speakers and industry experts participating in an Information Security risk management curriculum. Outliers refers to individuals entering the course without an IT degree. (ISLA Winner: Jennifer Chermoshnyuk, November 15, 2016) Based upon the student centric KBG model, adult learning theory and Bloom's Taxonomy, mid-career professionals mesh their industry specific knowledge with Information Assurance principles transitioning into positions of influence as cybersecurity concerns are being recognized across industry sectors. (Pental, 2017) Talented mid-career professionals from health care, law, logistics etc. recognizing the demand for a nationally recognized certificate in Information Assurance within their fields and gravitate to the program offered in-class and synchronously on-line.

The professionalization process of 'finding your swim lane' is also embedded into a current pilot in cooperative cybersecurity learning designed to close the gap between university/college graduation and acceptable professional performance on the job. Industry professionals acknowledge 'new' cybersecurity hires traditionally require 12 to 18 months' acclimation, workplace orientation and professional development before becoming strong contributors in the face paced cybersecurity workplace.

3 PROPOSED SOLUTION

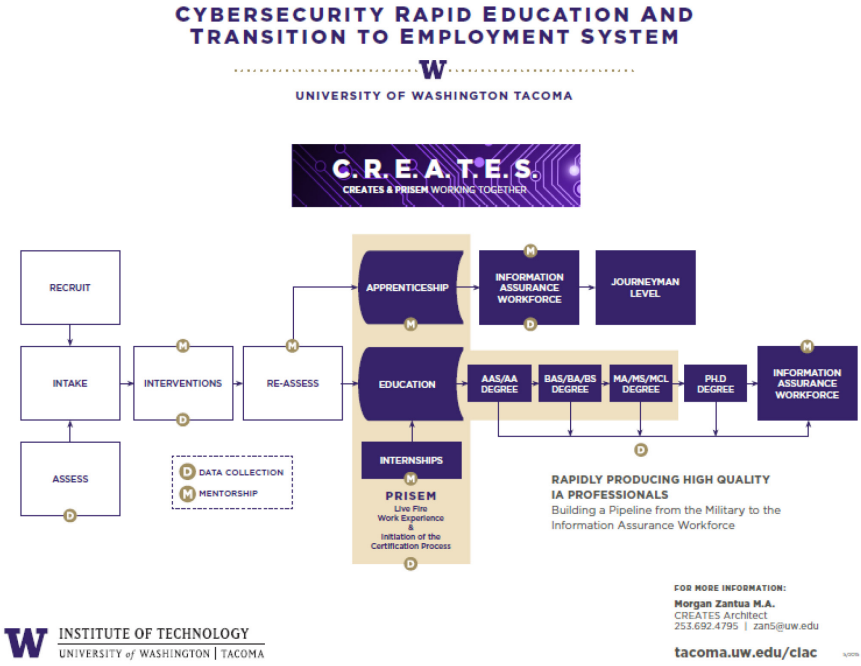
The proposed solution to increasing the flow of individuals entering the ever increasing and diversifying cybersecurity professionals is the customization of a statistically validated multi-dimensional career assessment tool and career guidance protocol for broad distribution. Outreach to candidates from all stages of career development is aimed to identify those well suited to enter the cybersecurity field. A multilevel career focus can significantly address the number challenges corporate recruiters face due to widespread digitization.

Modeling elements within cybersecurity after the medical concepts is not uncommon. Implementing a systems theory approach, computer systems and human systems are subject to viruses and consist of multiple interrelated systems. From an antedoctal perspective, after administering over 350 assessments to individuals interested in cybersecurity, interesting trends in the Career Recommendation emerged. As expected a high percentage of candidates received recommendations at the bachelor degree level for Computer Network Architect, Data Base Manager and other IT related disciplines. Another segment of individuals received Epidemiology and Marriage Counselor as career recommendations.

Our research team proposes to implement a research study based upon the methodology engaged to develop psychological profiles of surgical residents well suited to working in the Maricopa burn unit. Current research preparations are underway to engage cybersecurity professionals working in corporate, government and military settings. One hundred and twenty individuals engaged in two distinctly different career pathways will be assessed with the career guidance instrument referenced earlier in the paper. Anonymized data tagged with organizational performance indicators will be normed to establish a post-dictive performance profile combining 34 variables arranged in three specific categories. In additional to five sub categories within career training potential, 12 categories within job satisfaction indicators combined with 17 career interest subscales.

4 CASE STUDIES

During the return of soldiers from Afghanistan and Iraq, an international collaboration with the British Columbia Institute of Technology (BCIT) addressed transitioning Canadian veterans into post-secondary programs. Utilizing several assessment tools, specifically the WOWI, and career guidance to interpret career recommendation reports with coaching sessions "led to the conclusion that a majority of the soldiers had both the ability and suitability to be successful as advanced placement students in business diploma programs. (Wainwright, Spring 2015) Without this intervention these veterans intended to return to lower paying security work and laborer positions in their hometowns foregoing the opportunity of obtaining professional degrees.



Over the course of three years the university research and workforce collaboration resulted in a model constructed to establish a pipeline of transitioning military personnel into cybersecurity careers. The model, Cybersecurity Rapid Employment Academic Training Employment System (CREATES), received funding to conduct outreach during the troop draw down of 2014-15. (Zantua, 2015) Funding supported outreach to 234 service members transitioning out of the military through the Soldier for Life program. Fifty percent (112) indicated an interest in cybersecurity careers, 176 completed the assessment tool and 100 veterans were tracked entering undergraduate and graduate level cybersecurity education programs. (Seifer, 2016). Current funding opportunities expand CREATES to target additional populations. RECREATES is the Reserve (US Army) Expansion of the CREATES model. Honing cybersecurity talent within the Reservists' ranks has strong workforce ramifications. Reservists are civilians the majority of their workdays, called to serve during time of the emergency and provide strength to Active Duty forces. Cybersecurity is identified internationally (Charlaff, 2014) and nationally as the new battleground. A current research project studies the impact of Cooperative Learning, CoCREATES, on ten university students engaged in work experience opportunities with a major telecommunications corporation.

5 EVALUATION

Two con-current research projects, CoCREATES and RECREATES, recently approved by the Institutional Review Board study16 US Army Reservists and 10 undergraduate/graduate students participating in a work experience as a pathway to employment with a major telecommunications corporation. The research focuses on methodologies to close the skills and knowledge gap and shorten preparation time of cybersecurity professionals. Built into the project design is a panel of nationally recognized experts comprised of representatives from two and four-year academic institutions, industry and military. The panel's guidance and insight will inform a flexible replicable model attractive for adaptation at other colleges and universities working to meet the increasing demand for cybersecurity professionals. A university based evaluator has been involved since the inception of the program.

6 DISCUSSION AND CONCLUSION

What are the implications of customizing an instrument to build statistically valid psychological and talent profiles of professionals successfully engaged in cybersecurity roles? Using these profiles would it be possible to identify potential cybersecurity talent from different sources and more diverse populations?

Defining and standardizing cybersecurity professionalization is a work in progress. This paper does not address industry certifications and work being done by professional organizations. Efforts are underway through the Center of Academic Excellence system to build in curricular standards and reach out to the K- 12 community[1] while a guide to current cybersecurity career pathways is out for comment to the community (Newhouse, 2016). Both initiatives are worthy efforts. Speaking with academic leaders in the field in the past decades' students have 'self-selected' themselves to enter cybersecurity. Whether it was the 12-year-old hacker or today, the student attracted to the 0% unemployment rate for cybersecurity professionals, (Pental, 2017), there are no definitive psychological talent profiles for this rapidly emerging profession. It is unchartered territory.

Through work conducted since 2009, having a multi-functional career/aptitude/psychological assessment tool coupled with a strong career guidance and coaching process is a gap in the system requiring attention. By multi-functional we refer to a tool capable of identifying aptitude, temperament and career interest to high school students deciding upon post-secondary career options, college students identifying a major related to their career future, adults transitioning between careers; and organizations seeking to attract new talent, identify and prepare incumbent workers for their cybersecurity workforce. Informed career

[1] https://www.nsa.gov/resources/students/summer-camps/gencyber/

decision making being when coached by a workforce development professional lays a foundation.

Defining profiles of two distinctly different career pathways is the first objective. Based upon the results of post-dictive assessments, the team and the evaluator will be in a position to compare and contrast the similarities and differences between the two career pathways. Conversations with corporate partners to identify high demand and dissimilar pathways are underway. Further profiling of additional cybersecurity career pathways would be contingent upon the differences discovered through the initial psychological profiles and future funding. A cybersecurity focus coaching protocol is the second objective. Guidance counselors, coaches and human resource professionals trained in delivery of cybersecurity career development protocols will benefit the organization and the individual. Understandably, not everyone will have a cybersecurity career oriented profile but trained professionals armed with insights from a targeted tool can identify and nurture people with a propensity for cybersecurity career pathways. In the course of this nurturing, the mere mention of the diversity of careers in cybersecurity could help close the gap in the supply and demand of people entering the field. Cybersecurity career development is currently behind the curve in this rapidly emerging field. The initial work proposed, research based assessment tools and coaching protocols, can lay a foundation for outreach across populations to identify undiscovered talent.

7 FUTURE WORK

Dissemination of results defining the outcomes of the cybersecurity career profiling initiative comes next. Presenting results and protocols at targeted conferences to share the cybersecurity psychological profiles research includes an invitational challenge to corporations, high schools, colleges, universities and transitional worker programs to implement the assessment/coaching protocol. Included in the invitation is the suggestion to consider collaborative long-term cybersecurity career studies measuring the impact of identifying cybersecurity career profiles in candidates provided by the assessment and career guidance counseling.

Application of initial cybersecurity/psychological profiles will be incorporated into program recruitment protocols. Further validation of profiles will inform future profiling initiatives to other cybersecurity career pathways.

REFERENCES

[1] Burley, D. E. (2014). Would cybersecurity professionalization help address the cybeersecurity crisis? ACM, 24-27.

[2] Burning Glass Technologies. (2015). *Job Market Intelligence: Cybersecurity Jobs, 2015*. http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf.

[3] Charlaff, J. (2014). Cyberspace: The New Battleground. A Perspective from Israel. *Homeland Security Today.us*, pp. http://www.hstoday.us/columns/critical-issues-in-national-cybersecurity/blog/cyberspace-the-new-battleground-a-perspective-from-israel/1a663de30bef13199d8bf8be34f9a648.html.

[4] Endicott-Popovsky, B. P. (March 2014). Application of pedagogical fundamentals for the holistic development of cybersecurity professionals. *ACM Inroads*, 57-68.

[5] Evans, K. R. (2010). *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters*. Center for Strategic Initiatives.

[6] Foster, K. N.-R. (2010). A Psychological Profile of Surgeons and Surgical Residents. *APDS Spring Meeting*.

[7] ISACA. (2017). *State of Cybersecurity 2017: Current Trends in Workforce Development*. https://www.isaca.org/cyber/Documents/state-of-cybersecurity-2017_res_eng_0217.pdf: ISACA.

[8] ISLA Winner: Jennifer Chermoshnyuk. (November 15, 2016). http://www.itsecuritynews.info/isla-winner-jennifer-chermoshnyuk/.

[9] Johnson, N. (2015). The Air Force has a plan for testing cyber aptitutde. *Gov Loop*, https://www.govloop.com/the-air-force-has-a-plan-for-testing-cyber-aptitude/.

[10] National Science Foundation. (April 2009). *Veterans' Education for Engineering and Science: Report of the National Science Foundation Workshop on Enhancing the Post 9/11 Veterans Educational Benefit*. http://www.nsf.gov/eng/eec/VeteranEducation.pdf.

[11] Newhouse, B. K. (2016). *NICE Cybersecurity Workforce Framework (NCWF)*. NIST, US Department of Commerce.

[12] Pental, S. (2017). 10 New Information Security Roles for the Digitization Era. 24-26.

[13] Reich, D. U. (1999). The relationship of cognitivie, personality, and academic measures to anesthesiology resident clinical performance. *Anesth Analg.*, 1092-1100.

[14] Seifer, A. (2016). *Matopma; Omstotite pf Standards and Technology Technical Progress Report*. NIST Award No 60NANB14D229.

[15] Suciu, P. (2015, Sept 9). Cybersecurity's ever-growing brain drain. *Fortune Tech*, pp. http://fortune.com/2015/09/09/cyber-securitys-ever-growing-brain-drain/.

[16] US Department of Homeland Security. (2016). *Cybersecurity Workforce Development Toolkit: How to Build a Strong Cybersecurity Workforce*.

[17] Wainwright, K. F. (Spring 2015). An Alternative Approach to Prior Learning and Advanced Placement in Post Secondary Programs for Veterans. The Canadian Experience. *The Colloquium for Information System Security Education Special Edition: Educational Approaches to Transition former Military Personnel into the Cybersecurity Field*, 12-34.

[18] Zantua, M. D.-P. (2015). Re-Engineering the Cybersecurity Human Capital Crisis: *Educational Approaches to Transition Former Military Personnel into the Cybersecurity Field Special Edition of the Colloquium for Information System Security Education (CISSE)*, 156-152.