Searching and Developing Cybersecurity Talent

Barbara E. Endicott-Popovsky
endicott@uw.edu

University of Washington
Seattle, Washington

Viatcheslav M. Popovsky
dr_popovsky@hotmail.com

University of Idaho
Moscow, Idaho

Abstract - The lack of talent in the field of cybersecurity is keenly felt across all sectors of the economy - industry, government, military, academia [1]. While cybersecurity education has been a national priority, there still are thousands of cybersecurity jobs going unfilled and the gap will take a long time to close [1]. Of further concern, the authors have gathered anecdotal evidence that employers in both government and industry consider many recent cybersecurity graduates woefully unprepared for the realities of the workplace, taking too long to become effective. This paper describes one university's approach to address both the supply and preparedness problems, beginning with the application of the theory of pedagogical systems and methodology from sport and physical culture science and pedagogy to introducing the first iteration of a cooperative learning model - inspired by this theoretical base and experience with its application - designed specifically to develop and graduate 'breach-ready' cybersecurity professionals.

Categories and Subject Descriptors

K.3.2 [Computers and Education]: *Computers and Information Science Education*

General Terms

Cybersecurity education, pedagogy, cooperative learning

Keywords

Cybersecurity talent selection, pedagogical system, career development, cooperative learning pilot program

1 INTRODUCTION

Responding to the well documented deficit in cybersecurity talent in the U.S. [1], the Center for Information Assurance and Cybersecurity (CIAC) at the University of Washington, an NSA / DHS CAE-CDE, has created a unique laboratory for unleashing student potential by leveraging the interdisciplinary science and system-activity approach ingrained in the theory and methodologies of physical culture science and advanced sports pedagogy and applying that construct to cybersecurity education [2]. This scientifically-proven sport talent search system, developed by such luminaries as V.M. Zatsiorsky, N.G. Bulgakova, U.F. Kuramshin, and etc., allows individuals to find their appropriate physical activity aligned with their level of performance, authentic nature, and unique abilities [3, 4, 5, 6, 7]. This inevitably leads to superior performance and a fulfilling sport career, culminating in the athlete's personal happiness and sense of well-being.

Historically, sport orientation and selection science were rooted in psycho-physiological research from professional orientation studies, especially for selecting those for high risk, stressful, performance-demanding careers like airline pilot, special-forces military, and air traffic controller. The authors hypothesized that the field of cybersecurity, being similarly stressful,[1] would benefit from the application of this same research and have spent over a decade in actualizing this idea through

[1] One CISO, Chief Information Security Officer, from a major local firm indicated that after 3 major incidents employees need a sabbatical to recover!

individual courses and programs, writing extensively about their results in numerous publications referenced in [2]. The synthesis of that work into a repeatable methodology, and the initial draft of a cooperative learning model designed to address developing and producing 'breach ready' graduates, is discussed in this paper.

2 COMMON FACTORS FOR DEVELOPING TALENT

Studying the development of athletic talent through the work of physical culture educators [3, 4, 5, 6, 7], the authors identified four common factors that are applicable to achieving success in any field and have applied them to their cybersecurity education programs:

2.1 Factor 1 - Talent Search Process

Talent search is a continuous process, not a single event. Once talent is identified and selected, it must be continuously developed in a process that unifies nature and nurture described by W. Kistler, Founder of the Foundation for the Future [7]. Kistler suggests that nature and nurture co-exist in successful individuals as a 'unity of multiplication.' Attention to both in the talent search process amplifies growth and development.

The authors have applied this concept to developing an approach that helps students select their ideal cybersecurity career pathway that leverages their nature - in-born skills / abilities - with an appropriate plan to nurture those talents through continuous mentoring. An example of one of the tools used in this approach is the National Initiative for Cybersecurity Education (NICE) framework, [2] US National Institute of Standards and Technology (NIST) which provides guidance regarding necessary knowledge, skill, and abilities (KSA's) required for 32 different career pathways in cybersecurity. Their students are asked to identify pathway/s that resonate with their interests, do a gap analysis with their current conditions and design a way forward to eliminate those gaps with a professionalization plan augmented with continuous mentoring from professionals and staff which direct

[2] Found at http://csrc.nist.gov/nice/index.htm

students to free online courses and resources to fill in any gaps they may discover based on assessments provided each student.

2.2 Factor 2 – Intense Personal Interest

An athlete's passion for their chosen sport is accompanied by a desire, almost a craving, to work enthusiastically hard on self-improvement, allowing them to succeed and flourish in their field. The authors share the opinion of some researchers [5, 7, 8] that a person's commitment to persevere, in spite of obstacles, and their resilience to overcome setbacks in order to strive for their dreams are a reflection of their internal nature. In other words, intensity to succeed works from the inside out, leveraging passion and predisposition to a preferred activity.

In cybersecurity education programs at the Center for Information Assurance and Cybersecurity (CIAC),[3] students are offered a wide array of outside professional activities to experiment with finding their passion in cybersecurity and are encouraged to take multidimensional career assessment tests that measure interests, skills and work styles to help them identify what they like to do and what they are good at doing. These activities focus students on finding their ideal pathway in cybersecurity. When a student is passionate about their choice they become dedicated to learning - a basis for becoming a lifelong learner which is essential for success in this fast-moving field. Passionate students join cyber competitions, spend extra time on homework and seek mentors - all of which accelerates their learning and growth.

2.3 Factor 3 – Individualized Approach to Coaching and Mentoring

The availability of willing coaches and mentors who provide personalized individual feedback for continuous improvement - both good and corrective - additionally accelerates an athlete's growth.

[3] These programs are available for dissemination to other interested cybersecurity educators.

For the cybersecurity student in the Center's programs, mentoring is designed-in through a professional development service that works with students individually to partner with industry and government that provide advising, monitoring, and feedback throughout the learning experience. The authors are in the early stages of exploring ways in which the labor-intensive nature of this process can be reduced so significant scaling is possible.

2.4 Factor 4 – Well-structured Nurturing Pedagogical Process

Integrating highly motivated individuals (students, athletes, professionals) into a valid cooperative and competitive educational environment, combined with a well-designed pedagogical progression for achieving measurable personal (and team--in the case of sports) goals, accelerates an athlete's learning and improvement.

Applying this factor to cybersecurity education, a pedagogical process has been developed that combines work in the real world with existing studies in one of several academic degree programs and professional certificates designed to move students in planned stages from textbook knowledge to advanced problem solving of current cases presented by role model practitioners. Assignment assessments often include practitioner feedback, providing students measurable results that can reassure them of their developing competency.

This pedagogical system, designed to produce cybersecurity professionals, views incoming students as raw material to be processed! A unique blending of pedagogical approaches [9, 10, 11, 12], Figure 1 represents the pedagogical process that produces cybersecurity expertise as the outcome. This operational pedagogical system is derived from intensive research into two schools of thought regarding the theory of pedagogical systems whose originators are Drs. N.V. Kuzmina and V.P. Bespalko, respectively.[4] This is a high-level metasystem that, when applied to developing a specific course or program, produces a specific instantiation, many of which have been published as described in [2].

[4] In acknowledgement, the authors named the model KBP (Kuzmina-Bespalko-Popovsky).

KBP is composed of five elements - *students*, *teachers*, *goals*, *content* and *didactic processes* - the first two are intelligent elements, the *teacher* and the *student*; the remaining three are infrastructure elements - the *goals*, *content*, and *didactic processes* of the curriculum. All elements are subject to varying rates of change and adaptation over time requiring that programs continually update. All elements function as an integrated whole and operate within a larger dynamic environment with constantly evolving threats, vulnerabilities and technical innovation. Context informs the elements of the model.

In any given context, a specific instructor with their own specific slice of cybersecurity expertise is responsible for organizing content and selecting didactic processes designed to address the needs of students who are central to the pedagogical process. The orientation of the instructor will affect content delivered and didactic processes engaged. Students enter the learning experience with potential, and graduate with a professional orientation.

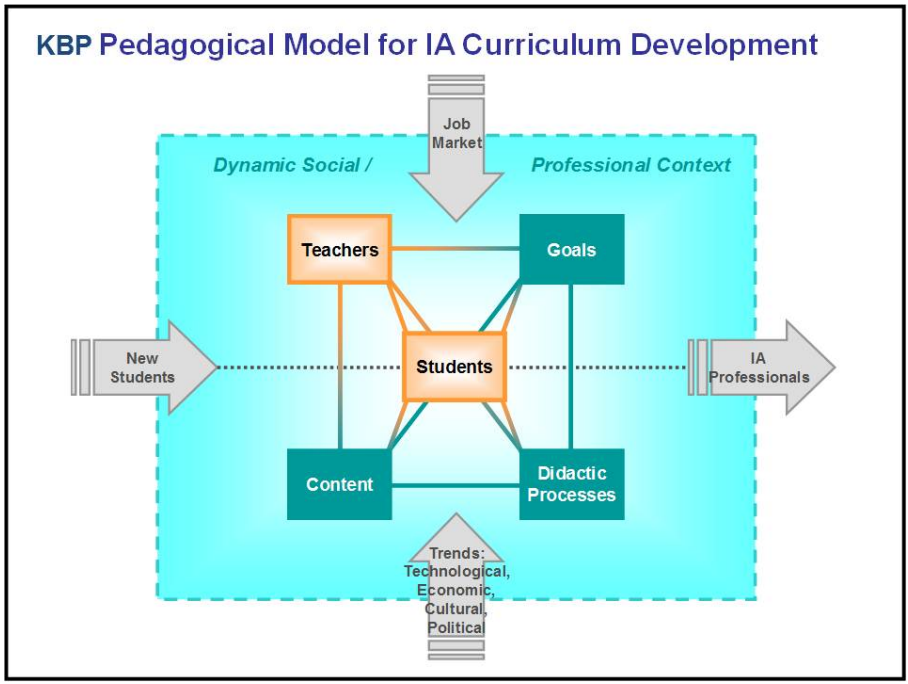

Figure 1: The KBP Pedagogical Model for Production of Cybersecurity Professionals

By describing each component of the model in relation to goals drawn from the current context, an educational plan is developed, iteratively. According to Bespalko and Kuzmina, the more precisely the five components are characterized - along with the connections among them - the more repeatable and predictable the learning results [9, 10].

Over time, as context changes, the entire system is affected, as well as any resulting curriculum. Each element must be re-defined with any update until all five are specified in relation to one another. By continuously updating the curriculum in this manner, students are kept current and graduates remain competitive. It is also an efficient approach to curriculum maintenance in a constantly changing field.

The Didactic Processes element deserves particular attention. The authors incorporate an activity-based learning approach developed in partnership with the regional cybersecurity community, academic researchers, and industry [13]. Since emphasis is placed on professional development, students are encouraged to learn from every possible resource: educational partners throughout the State, certifications, the Center's vast network, professional memberships. Knowledge is treated, not as an end goal in and of itself, but rather as a tool for solving real world problems, creatively and independently. Tools need continual sharpening.

A major feature of curriculum design is integration of cybersecurity practice into student experience everywhere possible. Active incorporation of this perspective helps students triage between the classroom and the real world so they can solve problems creatively, as opposed to applying a checklist from a book. Techniques for accomplishing this include:

- Recruit recognized cybersecurity experts as instructors.
- Employ guest lecturers for currency, role models, and job sources.

- Incorporate capstone projects from industry and academic research to develop problem-solving capabilities in students.
- Offer internships so students can immediately apply what they learn.

The end result is production of critical thinkers who are able to reflect on practical experiences, extrapolate generalizations through induction—extending their knowledge. Criteria for measuring results include students' contributions to science and industry.

3 RESULTS OF APPLYING THE KPB MODEL

The supply deficit of adequate numbers of skilled cybersecurity professionals is a well-recognized problem.[5] For more than ten years, the authors have applied the above four factors to this problem in order to develop sufficiently trained, ready-to-work, professional cybersecurity graduates. The educational approach that the authors created has a proven track record for producing talent in significant quality and quantity to have earned national recognition.

University of Washington programs following this approach have consistently earned a top-10 ranking in cybersecurity education from various authorities in the field [14]. Further, one of the programs, a professional certificate,[6] has earned US Western Regional awards from the University Professional and Continuing Education Association (UPCEA) for teaching and curriculum / pedagogy, as well as numerous individual teaching awards for instructors. More importantly, over 600 students have graduated from this one certificate program, alone, many of whom have now moved into senior management ranks and are reaching back to hire program graduates.

[5] There are many studies that confirm an extreme deficit of needed cybersecurity talent. For this paper, the authors refer readers to the following 1) Cybersecurity skills gap: https://securityintelligence.com/five-must-read-articles-on-the-cybersecurity-skills-gap/ and 2) Burning Glass study: http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs.

[6] The Information Security and Risk Management (ISRM) certificate.

The authors have relied on physical culture and sports pedagogy research to identify those factors that enhance talent development and have applied them to the forming profession of cybersecurity. The results have demonstrated the efficacy of transferring physical culture science and pedagogy to another field.

4 COOPERATIVE LEARNING PILOT

Recently, the Center has moved beyond internships to develop a cooperative learning[7] pilot in partnership with local industry which extends the pedagogical model (Figure 2) where the original KBP Pedagogical Model overlays a repeat pedagogical model, consisting of the four-elements from the employer's view representing the coop program. The fifth element, students, is the same for both layers of the model.

[7] By cooperative learning, the authors mean a structured approach that combines classroom-based education with practical, aligned experience in a real-world environment.

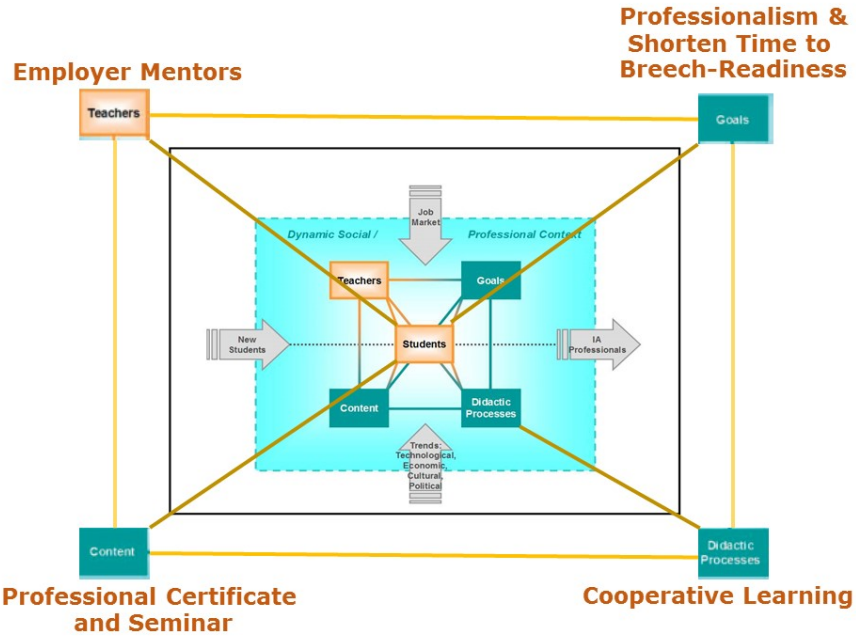

Figure 2: The KBTP Pedagogical Model in Partnership with Employers

The didactic process of incorporating cooperative learning in the student's employment is structured to address the goal of shortening the time to 'breach-readiness' through the active involvement of employer mentors and content from a professional certificate and seminar.

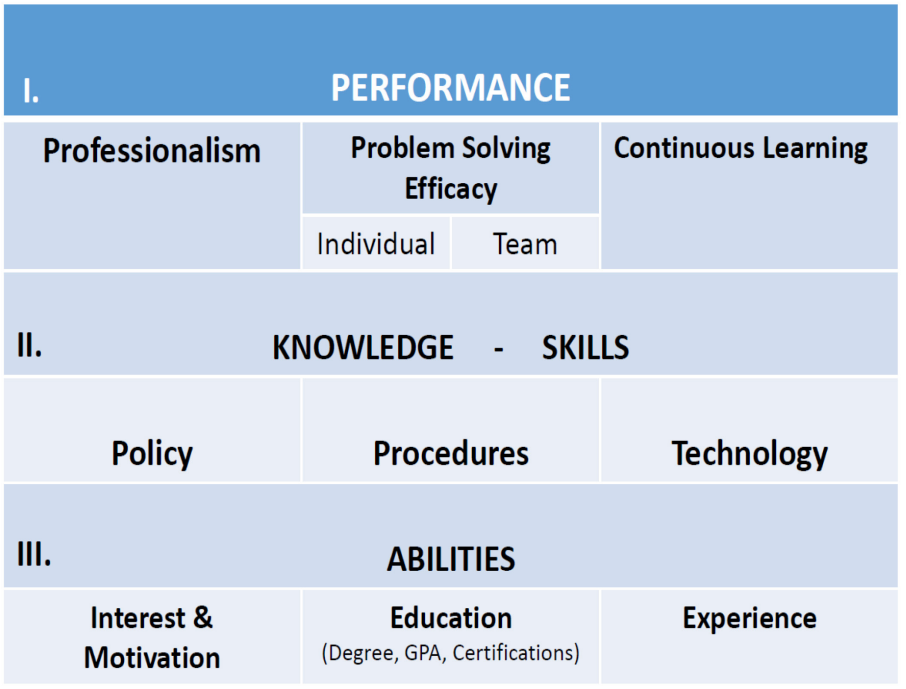

Figure 3: Cybersecurity Professional Readiness Model (CPRM)

Another stated goal for this expanded pedagogical model is achieving professionalism as defined in Figure 3. There are three dimensions of professionalism developed in any Center program. (Professional preparation is the reason given for naming the Center among the top 10 best places to study cybersecurity in the nation in 2014 [14].) These are:

- *Performance* is defined as exhibiting professionalism and problem-solving efficacy on the job, and indulging in a program of continuous learning.
- *Knowledge-skills* acquisition is defined as understanding policy development and implementation and effective application of procedural and technological controls—the 'rules and tools' of cybersecurity.
- *Abilities* as evidenced by the following: a student's interest and motivation, their educational accomplishments and their experience—especially

experience relevant to cybersecurity and the level of responsibility they have attained.

Application of the Cybersecurity Professional Readiness Model (CPRM) could be applied as a measuring instrument and can guide careers toward preparation for positions at the operating, managerial or executive levels, as well as identify gaps in preparedness, so that they can build plans to eliminate and compensate for any deficiencies. This is both a tool for selection and continuous guidance.[8]

Figure 4: Cybersecurity Cooperative Learning Pilot

[8] CPRM is derived from the work of a Russian sports pedagogical research group who used these three levels—Performance, Knowledge/Skills, and Abilities—for managing and selecting high performance athletes. The authors have adapted and applied this model for the selection and management of cybersecurity talent [15, 16].

Combining the models in *Figures 2* and *3*, the authors devised a cybersecurity cooperative learning pilot (*Figure 4*) where students maintain their current academic load in the last year of their degree programs and, in addition, opt into an integrated program of professional instruction and half-time industry employment. The additional professional education includes: 1) an information security and risk management (ISRM) certificate that covers all the necessary KU's required of a CAE-CDE and 2) a professional seminar conducted by the university in partnership with industry to help students triage their work experience with what they've learned formally in the classroom. The addition of the professional seminar and certificate elements in the pilot are expected to accelerate student work readiness when they formally graduate and give students the opportunity to reflect on what they are learning in the classroom and learning on the job, including teamwork, and the experience of adjusting to the working world. Table 1 provides an overview of the pilot program for AY 2016-17.

Cooperative learning program 2017		
Quarter	**UWB CIAC contributions**	**Employer contributions**
Fall 2016	▪ Recruit students (4 Business, 4 STEM), assess proficiencies, create individual plans for meeting requirements. ▪ Establish cohort ▪ Establish assessment and review process for the cooperative learning program.	▪ Participate in selection of students and establishment of cohort ▪ Participate in plan for program assessment and review

Cooperative learning program 2017		
Quarter	**UWB CIAC contributions**	**Employer contributions**
Winter 2017	▪ ISRM-1: *Business context for cybersecurity*. ▪ Fulfilling ISRM prerequisites ▪ Host cohort meetings	▪ On-site 0.5 FTE employment ▪ Host cohort meetings
Spring 2017	▪ ISRM-2: Risk management. Capstone course (for some) ▪ Host cohort meetings	▪ On-site 0.5 FTE employment ▪ Host Professional Development Seminar
Summer 2017	▪ ISRM-3: Solving problems. ▪ Award ISRM certification. Capstone course (for some students) ▪ Program review and assessment ▪ Host cohort meetings	▪ On-site 0.5 FTE employment ▪ Host Professional Development Seminar ▪ Participate in program review and assessment

Table 1. Cooperative Learning Pilot Project Plan

5 CONCLUSION AND FUTURE WORK

In addition to support from industry, government is also a partner in this pilot. The National Information Assurance Education and Training Program (NIETP) is interested in the development and dissemination of the cooperative learning model and the lessons learned during the pilot period. This is conceived as a two-year pilot. This first year 10 students, constituting one cohort, are engaged with one employer. Students were selected based on technical foundation, interpersonal skills, team participation, and collaborative problem-solving. ISRM certificate scholarships were provided. A second year of the pilot will be conducted with more industry partners for the purposes of incorporating lessons learned from the first year and refining and generalizing the model.

In the second year, 2 new industry partners will be added to test the ability of the program to scale allowing for 3 cohorts of 10 students each. Recruiting is planned for Summer 2017 with admittance into the pilot for AY 2017-2018. The professional education elements will run in three consecutive quarters, this year beginning in Fall 2017 – Winter 2018 – Spring 2018. The data collected will provide insight into several questions: 1) whether / how this program will / can be scaled, 2) whether this kind of a program accelerates cybersecurity job readiness, 3) what are best practices for conducting such a program.

REFERENCES

[1] Burning Glass. Job Market Intelligence: Cybersecurity Jobs (2015). Retrieved April 15 at: http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf

[2] Endicott-Popovsky, B. and Popovsky, V. Application of pedagogical fundamentals for the holistic development of cybersecurity professionals. ACM Inroads, 5(1), 57-68 (2013).

[3] Yakhontoff, ER. Didactical reformation of the content of athletic and pedagogical coaching activities in sports games. Autoreferat of Diss., Lesgaft Academy, St. Petersburg: Russia, (1995).

[4] Popovsky, V. The System of Continuous Pedagogical Practice in IPC. S.P Evseev and Popovsky, V. (Ed.) Organization and Methodology of Continuous Pedagogical Practicums in the Institute of Physical Culture: Academic Methodological Benefits, Leningrad: Lesgaft Institute of Physical Culture (1988).

[5] Kuramshin. U.F. and Popovsky, V. Find your Talent. Leningrad: Lenizdat (1987).

[6] Ageevec, V.U., Popovsky, V., Filippov, S.S. The Mini–Department of the Institute of Physical Culture–A New Form of Student Work. Theory and Practice of Physical Culture, Moscow: Russia, No 11 (1984).

[7] Il'in, E.P. Psychophysiology of Physical Education. Prosvetshinie: Moscow, Russia (1980).

[8] Kistler, W. Reflections on Life. Presentation: Foundation for the Future: Bellevue, WA (2003):

[9] Kuzmina, U. F. Fundamentals of Pedagogy of Higher Education. Leningrad: Lenizdat (1972).

[10] Bespalko, V. P. Fundamentals of Theory of Pedagogical Systems. Voronege: Voronege University (1977).

[11] Bloom, B.S., Mesia, B.B. and Krathwohl, D.R. Taxonomy of Educational Objectives. New York: David McKay 1964).

[12] Hutton, G. Backward curriculum Design Process. Retrieved May 1, 2003 from the World Wide Web: http://www.g4v.com/~glen.hutton/ED3601/BackwardDesignFeb11_03.pdf

[13] Endicott-Popovsky, B. and Popovsky, V. Activity-based approach to developing professionals within higher education programs. 1st Annual Conference at the

Department of Physical Education. St. Petersburg, State Institute of Film and Television. St. Petersburg, Russia (2015).

[14] [Ponemon Institute. 2014 Best Schools for Cybersecurity (February 2014). http://www.hp.com/hpinfo/newsroom/press_kits/2014/RSAConference2014/Ponemon_2014_Best_Schools_Report.pdf

[15] Kuznetsov, V.V. Novikoff, A.A. To the Problem of Modeling the Characteristics of High Performance Athletes. Theory and Practice of Physical Culture. Vol.1. Moscow, USSR. pp. 50-62 (1975).

[16] [Shustin, B.N. and Bryankin, C.B. Using "Models of High Performance Athletes" for Selection and Sport Orientation. Proceedings of Problems of Selection of Young Athletes. Moscow, USSR. pp. 11-13 (1976).