Applying Competency-Based Learning Methodologies to Cybersecurity Education and Training: Creating a Job-Ready Cybersecurity Workforce

By Alan B. Watkins, David H. Tobey, Ph.D., and Casey W. O'Brien

What do the Financial Services and Chemical sectors have in common with the Transportation and Government Facilities sectors? All sectors need workers skilled in cybersecurity. What will it take to have qualified workforce candidates coming out of education or training programs with the necessary cybersecurity skills and abilities? A global study indicates there will be a shortage of approximately 1.8 million skilled cyber workers in the next few years (Center for Cyber Safety and Education 2017).[1] *This creates a two-fold problem for national security and protecting our critical infrastructure from cyber attacks. First, is training a sufficient number of new information security workers and, second, is ensuring that existing Information Technology (IT) and cybersecurity workers have the requisite skills to provide necessary levels of security to protect information assets. This paper addresses the second issue – how to better equip learners to enter into, or remain in, the workforce with the necessary cybersecurity skills and abilities. This paper proposes the use of Competency-Based Education and Mastery Learning (CBML) methodologies as an innovative and more effective approach than the current Outcome-Based Education (OBE) approach. CBML methodologies strive for learners to master critical skills at a minimum 95% competency level, before moving on to the next knowledge or skill component; rather than the OBE approach, where a "passing" grade of "C" equates to a 70% competency level. From which approach would you want to hire cyber workers for the Healthcare and Public Health sector or the Energy sector?*

Introduction – What's the Problem?

Technology professionals, as well as business executives are aware of the continuing increases in cyber attacks against both large and small businesses, across all industries. Large data breaches have become somewhat common news items for both private sector companies and government agencies; where no one is immune from becoming a victim, whether in the Financial Services sector, Energy sector, Transportation sector or Information Technology sector. There are a few commonalities across all 16 of the critical infrastructure: first, they are all targets for cyber attacks, some with a higher potential to be attacked than others, and second, they all need qualified, skilled workers to help their organizations protect against and respond to cyber attacks.

This need for skilled cybersecurity capabilities in the workforce is creating a dual problem facing all of the critical infrastructure sectors. First, there is a well-documented shortage of qualified candidates to fill vacant cybersecurity positions. However, the focus on these specialized roles may be masking a much greater need – the adequate maturation of

[1] Frost & Sullivan. *2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, North America Executive Briefing*. Technology Industry Global Workforce Study: Executive Summary, Center for Cyber Safety and Education, 2017.

cybersecurity capabilities of all information technology (IT) professionals necessary to not only qualify them for those positions, but to also help them excel in performing security functions to protect our nation's critical infrastructure. Second, there is a need to ensure that the current and future IT workforce is able to maintain and enhance their skills, that more IT workers be qualified for promotion into specialized cybersecurity job roles, and that all workers keep up with advances in technology and more complex attacks. The need spans the private sector and all levels of the public sector – federal, state, local, and tribal. In addition, the size of an organization only matters in the sense that larger organizations need a larger pool of IT and cybersecurity staff; however, targeted attacks against small businesses (less than 250 employees) increased from 18% of total phishing attacks in 2011 to 43% in 2015 and, therefore, they also need cybersecurity services performed by qualified professionals.[2]

In the United States, there are hundreds of colleges and universities offering undergraduate and graduate degrees in cybersecurity and related fields, including 110 institutions [at the time of publication] designated as National Security Agency (NSA)/Dept. of Homeland Security (DHS) National Centers of Academic Excellence in Cyber Defense (CAE-CD).[3] There are also a wide variety of professional certifications available, which are intended to show a person's successful completion of specific training and a practical exam, indicating a level of proficiency in certain technical skills related to the certification. Some of the more common certifications include various offerings from the SANS Institute; the Computing Technology Industry Association's (CompTIA's) Network+ and Security+; the International Information System Security Certification Consortium's (ISC2's) SSCP (Systems Security Certified Practitioner) and CISSP (Certified Information Systems Security Professional); ISACA's CISA (Certified Information Systems Auditor) and CISM (Certified Information Systems Manager), and the International Council of Electronic Commerce Consultants' (EC-Council's) Certified Ethical Hacker (CEH). The vast majority of academic and training organizations rely on an outcome-based education (OBE) approach, and hiring managers are finding that applicants do not have the necessary skills and abilities to fill their cybersecurity positions.[4]

An alternative approach to teaching cybersecurity skills is needed to overcome the gap between the number of unfilled positions and the number of competent candidates. The innovative approach being proposed in this paper is to use CBML methodologies to produce a higher number of workers who are proficiently/competently skilled in cybersecurity. The CBML approach focuses on mastering each critical knowledge and skill component before moving on to the

[2] Symantec. *2015 Internet Security Threat Report (ISTR), Volume 21*. Annual Cybersecurity Trends, Symantec, 2015, 43.

[3] National Security Agency. *NSA/DHS National CAE in Cyber Defense Designated Institutions*. n.d. https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm (accessed June 8, 2018).

[4] ISACA. *State of Cyber Security 2017: Current Trends in Workforce Development*. Trends in Cybersecurity, ISACA, 2017, 9.

next one,[5] without being constrained to a fixed time period; rather than the current, OBE approach which attempts to teach several knowledge and skill components within a fixed time period and reach a "passing" score of competence. In the following discussion of these two approaches, the presumption is that the CBML approach will produce better results in qualified cybersecurity and IT workers.

This CBML approach can be applied to almost any area of training or education, including operations and security for Industrial Control Systems (ICS), such as Supervisory Control and Data Acquisition (SCADA) systems, used by the Energy sector, Chemical sector, Critical Manufacturing sector, Dams sector, Water & Wastewater sector, and Nuclear Reactors, Materials, & Waste sector. Using a customized CBML approach would mean having more qualified workers for the specialized systems which control critical equipment used for various industrial processes – for example, adding chemicals for water purification, controlling the flow of water over a dam spillway, managing the distribution of power between substations, or controlling the dilution of full-strength chemicals into consumer-grade products.

Outcome-Based Education Methodology – The Current Approach

Over the last century, standard teaching practices have primarily used an OBE approach to learning for almost all fields of study. This approach is typically based on Learning Objectives for a set of topics and is focused on teaching the curriculum materials within a fixed period of time (e.g., an academic quarter or semester in a school year, or a 40-hour/Boot Camp training course). The intent is to have as many students (or learners) as possible achieve a passing grade, usually a "C" for schools or 70%-75% for training programs.

The OBE approach is not without its benefits, otherwise it would not have been so widely adopted as a standard teaching methodology. It starts with a set of Learning Objectives which a learner must understand and achieve a passing level of proficiency upon completion of the academic class or training course. The curriculum or course content is developed, generally using a top-down approach, to teach the necessary knowledge and skills for the learner to understand the underlying principles and processes for each Learning Objective. The assessments (quizzes and exams) are evaluated on how many correct answers each learner achieves. The correct answers determine which students are selected to receive recognition in the form of grades, awards, and ultimately a credential (i.e., industry certification or college degree). The selective rating process results in a standard bell curve distribution where the majority of learners are within the average "passing" score, plus or minus one standard deviation – the high achievers and the low achievers fall into the next standard deviation above and below the primary group, respectively. OBE is a very efficient system of education that has excelled in providing access to higher education for most of the population while minimizing investment in teaching and

[5] *Mastery Learning Manual*. Johns-Hopkins University, n.d.

instructional resources. Accordingly, success in OBE is defined by the number of students completing a degree within a defined timeframe per instructional resource. Policy makers evaluate completion rates by institution while education administrators evaluate completion rates per department or faculty member. The metrics of success are credit hours earned and headcount per degree program.

While the OBE approach excels at breadth of learning, creating deep learning – raising the capability maturity – of every student has been challenging. There is less focus on meaningful understanding. There is no focused effort to go back and assess why a learner had answered questions incorrectly. An old saying that might apply to this approach is, "a Jack of all trades, but a Master of none;" since you might learn a lot of things about several topic areas, but you are not given the time or structure to become highly proficient in any one. The goal is for all of the content to be covered within the timeframe of the course, so that all Learning Objectives have been covered, regardless of whether all of the learners had the necessary time to gain proficiency in all of the knowledge and skills being taught. The primary OBE instructional resource, the textbook, is designed to broadly cover the topics within a domain. Many textbooks emphasize a survey of the long-accepted tenets of a discipline and eschew constantly changing or current trends in job-specific knowledge and skills. Accordingly, many learning objectives are broad but shallow. It is not uncommon for an entire course to have only several learning objectives, whereas performance on the job would require mastery of dozens of tasks. Furthermore, OBE methods do not ensure that learners have sufficient proficiency in core concepts before moving on to intermediate and advanced concepts. Assessments may provide important clues as to what a learner does not know or has not learned; however, as long as they correctly answered the minimum number of questions correctly, they are advanced to the next learning module or course. Unfortunately, those concepts not mastered by the learner create a cumulative effect. Nearly every student will lack proficiency in some topics and many may lack complete and confident understanding of most topics for each Learning Objective, starting with the basic, core concepts. Eventually, the gaps in knowledge lead to the learner's inability to properly grasp the more advanced topics that build upon those core concepts.

Competency-Based Education Methodologies – An Innovative Approach

A CBML approach, which the U.S. Department of Education (DoE) calls competency-based learning, and also personalized learning, favors "a structure that creates flexibility, allows students to progress as they demonstrate mastery of academic content, regardless of time, place, or pace of learning."[6] The U.S. DoE further states, "By enabling students to master skills at their own pace, competency-based

[6] U.S. Department of Education. *Competency-Based Learning or Personalized Learning*. n.d. https://sss.ed.gov/oii-news/competency-based-learning-or-personalized-learning (accessed June 8, 2018).

learning systems help to save both time and money. Depending on the strategy pursued, competency-based systems also create multiple pathways to graduation, make better use of technology, support new staffing patterns that utilize teacher skills and interests differently, take advantage of learning opportunities outside of school hours and walls, and help identify opportunities to target interventions to meet the specific learning needs of students. Each of these presents an opportunity to achieve greater efficiency and increase productivity."[7]

To start the process of defining competency-based learning materials, which could be used for either formal, academic education classes or industry-related training programs, there needs to be a validated list of competencies (primarily concepts and skills) relevant to specific cybersecurity functions and tasks. There are several repositories of cybersecurity jobs with their related requirements for knowledge, skills and experience; however, this proposal is based on the set of cybersecurity tasks, knowledge, skills, and abilities defined by the job performance models produced by the National Board of Information Security Examiners (NBISE)[8] and the competency model developed by the National Institute of Standards and Technology (NIST) and the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF), version 2, released in August 2017, as NIST Special Publication (SP) 800-181.[9] Created with broad public/private sector input, Appendix A of the NCWF lists work roles, tasks, knowledge, skills, and abilities (T/KSAs)[10] for various cybersecurity functions. While the work roles may not cover all private sector job or position descriptions, the NCWF is a good starting point for defined cybersecurity workforce standards. The NCWF starts by defining seven cybersecurity workforce Categories, broken down into 33 Specialty Areas with two to six per category, and defines 52 unique Work Roles within the Specialty Areas. Appendix A of the NCWF provides lists of approximately 1,000 Tasks (actions typically performed), 630 Knowledge items (what workers need to know about cybersecurity to perform job tasks), 370 Skills, and 175 Abilities. Appendix B of the NCWF lists each Work Role with its related Tasks, Knowledge, Skills, and Abilities, so that employers and prospective cybersecurity workers have a common understanding of the job requirements and the expected functions to be performed for each Work Role. The NCWF provides a descriptive framework while the NBISE job performance models enable predictive assessment of capability maturity. Together, the descriptive and predictive models aligned with a

[7] Ibid.

[8] O'Neil, L. R., M. J. Assante, and D. H. Tobey. *Smart Grid Cybersecurity: Job Performance Model Report*. Technical Report, U.S. Department of Energy, Alexandria, VA: U.S. Department of Energy, 2012.

[9] Newhouse, William, Stephanie Keith, Benjamin Scribner, and Gregory Witte. "NICE Cybersecurity Workforce Framework." Vers. 2.0. *NIST National Initiative for Cybersecurity Education (NICE)*. August 2017. https://csrc.nist.gov/publications/detail/sp/800-181/final (accessed June 8, 2018).

[10] Newhouse, William, Stephanie Keith, Benjamin Scribner, and Gregory Witte. *NIST Special Publication 800-181 NICE Cybersecurity Workforce Framework - Appendix A*. NIST Special Publication, National Institute of Standards and Technology, 2017, Appendix A, 11-94.

standardized cybersecurity curricula can provide the basis for developing CBML learning materials.

With the NCWF set of workforce Roles, Tasks, Knowledge, Skills, and Abilities providing a target for what a cyber worker needs to know and do, the next step is to develop Learning Objectives. Each learning objective should cover the applicable topics to address workforce requirements. Each Learning Objective consists of several topics which become the basis for learning modules. Designing and building CBML curriculum materials uses a bottom-up approach. The first step identifies the foundational learning objective topics, also known as threshold concepts (knowledge), actions (skills) or judgments (abilities). Passage across the threshold indicates mastery of prerequisite foundational expertise necessary to be ready to learn the intermediate topics. The intermediate topics must be mastered prior to moving on to the more advanced topics. Therefore, the emphasis of CBML is on learner readiness rather than completion. Each learner can complete their learning at their own pace and only when their performance has indicated that they are ready to do so. Whereas some OBE learning modules might be 45-60 minutes long and cover multiple topics, the CBML learning modules are shorter (i.e., 10-15 minutes) and focus on one or two closely related topics. An OBE course may have five or six Learning Objectives, each with five to ten topics or concepts to be taught using five to ten learning modules. On the other hand, one CBML course could have 50-100 Learning Objectives, each with dozens of topics or concepts with several learning modules for each Learning Objective. This level of detail allows grouping of related topics or concepts into a single learning module and enables more focused learning on the particular knowledge or skill. The CBML approach is ideal for personalized learning,[11] since the focus is on reaching a high level of competency and not on a timeline for each topic, several of which can be learned in parallel, not just sequentially. This approach counters the "Jack of all trades" notion and allows a potential information security worker to become a "Master of several trades."

Another step in developing the learning materials is properly grouping and sequencing the Learning Objectives into relevant courses, resulting in a matrix of courses by proficiency level (e.g., introductory, intermediate, and advanced) and by areas of specialization (e.g., information assurance, network monitoring, cryptography, digital forensics or penetration testing). At the base of this matrix will be a core set of foundational courses covering the threshold Learning Objectives which all potential cybersecurity workers must complete and master before moving into a specialization which, in effect, defines a learning pathway. Ideally, using links to the NCWF job roles with related tasks and KSAs, a potential cybersecurity worker should be able to trace a learning path from a desired job role and the needed knowledge and skills, through the CBML matrix, and create a customized education or training plan

[11] Lumina Foundation. "The Emerging Learning System." *Industry Trends*, 2016.

starting not necessarily at the foundational level, but at the worker's current level of competence. As stated earlier, this personalized learning path would benefit both current and future IT workers, as well as those seeking more specific cybersecurity jobs. In addition to being linked to the NCWF job roles, the Learning Objectives should be aligned with the Cybersecurity Job Performance Capability Maturity Model (JP-CMM) published by the Department of Homeland Security,[12] which would align the learning levels (introductory, intermediate, and advanced) with the workforce maturity levels (limited, progressing, and optimized) and also with the "Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity" issued by the ACM/IEEE Joint Task Force on Cybersecurity Education,[13] which will provide consistency across academic institutions.

As learning modules are being created using the CBML approach, a parallel effort needs to take place in developing continual, formative assessments – including pre-assessment questions, intramodule assessment questions, and post-assessment questions. The pre-assessment is intended to diagnose a learner's readiness to start the course. If the capability maturity is insufficient a differentiated learning path can be recommended to raise the maturity to prerequisite levels needed to ensure all the groundwork has been laid. Even entering the basic, foundational level for cybersecurity requires some background and knowledge of how computers function, differences in operating systems, basic networking concepts and protocols, and other general technology knowledge, which would be obtained in other education or training courses prior to embarking on a cybersecurity learning path. The intramodule assessments diagnose a learner's progress in achieving, or identify the obstacles to, sufficient proficiency within each learning module, such as certain process steps, before continuing with additional topics or concepts in a module. For example, in learning how to perform a vulnerability assessment, the module might start with basic network scanning techniques before actual vulnerability scanning. Post-assessments are given at the end of each learning module and again after completion of a Learning Objective (comprised of several modules), to ensure the learner has mastered development of the knowledge, skills and abilities needed to achieve that level of learning. A major difference between these assessments and the OBE approach, is that the CBML assessments focus at least equally if not more on the questions learners get wrong, to determine why they didn't get the correct answer. Consequently, CBML instruction can address directly any obstacle a learner faces to raising their capability maturity. For many years, studies have shown that this technique can raise the capabilities of most learners to that formerly attained only by the high achievers under

[12] U.S. Department of Homeland Security. "Cybersecurity Capability Maturity Model - White Paper." White Paper on Cyber Workforce, 2012.

[13] ACM/IEEE Joint Task Force. "Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity." Cybersecurity Curriculum Guidelines, 2017.

OBE.[14] Taking the time to provide the necessary clarification for incorrect answers, so the learners can understand and accept the rationale for the correct answer, is a valuable part of the CBML approach in achieving high levels of competency upon completion of a learning module or training course. Competence in this case, means mastering the knowledge or skill as close to 100% as possible, usually aiming for a minimum of 95%, which may require a learner to repeat all or part of certain learning modules, until reaching that level of proficiency, and before moving on to the next related or higher-level module.

Starting in the fall of 2017, National CyberWatch Center Curriculum Standards Panel participants have been developing CBML course materials for a single course: Information Security Fundamentals.[15] Curriculum design and development will continue with other IT and cybersecurity courses considered to be part of a Foundation Series of core subjects needed for those who want to embark on a cybersecurity career. After completion of the Foundation Series,[16] there will be Pathway Series courses at the intermediate and advanced levels leading to specific areas of specialization which may result in industry certifications or college degree programs.

Case Study: InfoSec Fundamentals Readiness Assessment

Several academic institutions and other organizations signed up to take part in a pilot of the Readiness Assessment created as a CBML tool to determine whether learners entering an Information Security Fundamentals (ISF) course have the prerequisite knowledge and skills necessary to successfully understand and learn the topics and concepts of the ISF course. As of June 21, 2018, there were 26 institutions participating in the Readiness Assessment, comprised of seven community colleges, nine 4-year universities, two technical trade schools, two international universities, five private organizations (i.e., non-profits), and one state Department of Education. As mentioned earlier, a CBML assessment is used to find out why a learner believes a wrong answer is correct, and then to provide instruction on the correct answer. At the time of publication, the pilot of the Readiness Assessment was just beginning, and results won't be known for several months, so instead, several participating registrants agreed to be interviewed. The interviews sought to find out why they decided to participate, what they expect from the results, and what benefits might accrue from using the assessment, for both students and their institution. The summary of responses are presented below, starting with some

[14] Bloom, B. S. "The 2 Sigma Problem: The search for methods of group instruction as effective as one-to-one tutoring." *Educational Researcher* 13 (1984): 4-16.

[15] National CyberWatch Center CSP. *Curriculum Standards Panel*. June 2018. https://www.nationalcyberwatch.org/csp/ (accessed June 8, 2018).

[16] National CyberWatch Center. *Certificate for Cyber Foundations Courses*. May 2018. https://www.nationalcyberwatch.org/programs-resources/curriculum/certificate/cyber-foundations (accessed June 8, 2018).

demographic information and excluding any Personally Identifiable Information.

The first interviewee is an instructor at the main campus of a small, regional technical/vocational college, with two dozen other campuses across the state, and which has three cybersecurity instructors. There are approximately 10 students participating in the assessment, out of 40 total on this campus, who are taking cybersecurity courses, all of which are on-site and self-paced.[17] The second interviewee is an instructor and also coordinator for distance learning at a medium-sized community college, which has twelve cybersecurity instructors. They will also have approximately 10 students participating, out of an annual enrollment of 6,000 students, and their cybersecurity program, consisting of six classes, uses a hybrid approach of both on-site and online classes.[18] The third interviewee is the director of education at another small, regional technical/vocational college which focuses on various IT and cybersecurity courses and certifications, with five cybersecurity instructors. There will be approximately 30 students participating, out of approximately 350 total annual enrollment and they also use a hybrid approach to their courses; however, they are in the process of migrating their cybersecurity tools to an internal lab environment linked with their internal LMS (Learning Management System). This means the classes will eventually be on-site only.[19] While the first three interviewees were all from an academic institution, the fourth and final interviewee is the vice president of information security at the parent non-profit organization which oversees a family of regional non-profit organizations (NPOs) across 20 states and two overseas offices, providing healthcare and social services, and certain veterans' services. This organization will have approximately 20 IT staff and 30 to 40 "cybersecurity champions" taking the assessment, which represents the current workforce as opposed to students.[20]

Beyond the demographic questions, there were four primary questions used to gather information – (1) reasons for participating in the assessment, (2a) current skill levels of participants and (2b) will assessment be used as a baseline for comparison with post-assessment after completing a training course, (3) how does the Readiness Assessment align with institution's cybersecurity program and does the institution use Competency-Based Mastery Learning methodology, and (4) reaction to how the assessment questions are formatted to capture the learner's level of confidence in their answer.

Each of the four interviewees have many similarities and some differences in how they are viewing the assessment and, of course, the whole perspective of the NPO differs from the three academic institutions. The two technical/vocational colleges have

[17] Mayberry, Joel, interview by Alan B. Watkins. *ISF Readiness Assessment Interviews* Nashville, Tennessee, (June 19, 2018).
[18] Smith, Aurelia, interview by Alan B. Watkins. *ISF Readiness Assessment Interviews* Alabama, (June 21, 2018).
[19] Hilario, Humberto, interview by Alan B. Watkins. *ISF Readiness Assessment Interviews* New Jersey, (June 21, 2018).
[20] Stevens, Dwayne, interview by Alan B. Watkins. *ISF Readiness Assessment Interviews* Nashville, Tennessee, (June 22, 2018).

similar goals of improving the effectiveness of their courses,[21] as evidenced by higher levels of student competence, with necessary operating knowledge[22] to be successful upon entering the workforce. Both view the Readiness Assessment as a pre-assessment of student skills and abilities which can help students determine a future learning path – for example, whether to move forward in cybersecurity or to focus on other IT functions (e.g., system administration). The community college sees the Readiness Assessment as a way to participate in NCC events and as part of their effort to become certified as a Center of Academic Excellence (CAE) school through the NSA/DHS.[23] Finally, in addressing the underlying reasons for participating in the Readiness Assessment, the NPO healthcare organization is seeking a baseline measurement for current IT staff and soon to be hired security staff, and sees it as a helpful tool in developing their internal security program.[24]

Across all four interviewees, they all report that approximately half of those who will be taking the Readiness Assessment have completed a security course (e.g., CompTIA's Security+), while almost all participants have completed a basic IT course (e.g., CompTIA's A+). Small numbers of participants have completed one or two security classes, but do not have certifications. There are, of course, those who have little to no past experience or training in cybersecurity and the first assessment will act as a baseline for future assessments to determine levels of competence and compare the amount of learning which occurred after the re-assessment. The first technical/vocational college already uses the CBML approach and has most students pass their courses with an "excellent" rating, meaning a 94% or higher score.[25] They would use the Readiness Assessment as a tool to validate student competence.

All interviewees agreed that the CBML methodology sounds like a good way for them to judge the success of their training and education programs, which aligned with their organizational goals; although the CBML methodology is not specifically used at the community college[26] or NPO,[27] it has been adopted at both technical/vocational colleges.[28] [29] As far as the format of the assessment questions, where the learner selects not just the correct answer, but indicates their confidence level in that answer, both technical/vocational colleges are familiar with and use this type of assessment format, which follows the CBML approach. The first technical/vocational college sees the assessments as an opportunity to address wrong answers and direct remedial learning for increasing overall competency levels.[30]

In closing comments: The first technical/vocational college plans to use this or similar assessments to continue moving in the direction of having higher levels of competence and assisting students in

[21] Hilario, Humberto, 2018.
[22] Mayberry, Joel, 2018.
[23] Smith, Aurelia, 2018.
[24] Stevens, Dwayne, 2018.
[25] Mayberry, Joel, 2018
[26] Smith, Aurelia, 2018.
[27] Stevens, Dwayne, 2018.
[28] Mayberry, Joel, 2018.
[29] Hilario, Humberto, 2018.
[30] Mayberry, Joel, 2018.

overcoming lack of knowledge in particular areas.[31] The community college was unsure about the current alignment of CBML, and believes it is the direction they should take.[32] The second technical/vocational college will continue its use of CBML to provide its students with the necessary skills to succeed in the business world.[33] Lastly, the NPO plans to use CBML to the best of its ability in building its security program, which includes employee training (IT staff, security staff, and security "champions").[34]

Conclusion

A growing number of employers report the lack of qualified workers with the necessary cybersecurity capabilities to protect and defend critical infrastructure. This paper argues that the failure of the current education system to deliver sufficient numbers of qualified workers may be addressed by applying recent developments in competency-based mastery learning methodologies. We discuss the detriment to the talent pipeline created by the current focus on students completing education and training courses with only a "passing grade." Many of these graduates lack the capability to achieve certification and meet employer needs. Instead, we advocate and describe a curriculum standards initiative that is applying CBML as an alternative to the traditional OBE approach. Our goal is to increase the number and deepen the capability of all information technology workers by replacing an educational system focused on selecting a group of high-achieving specialists.

About the Authors

Alan B. Watkins is an independent cybersecurity consultant and an adjunct professor in cybersecurity and information assurance at National University. In his prior career, Mr. Watkins worked for the City of San Diego in various positions for over 36 years, starting with 12 years in law enforcement and then 24 years in information technology (IT), including 10 years in management and his final 5 years as the city's IT Operations and Security Manager. He has been a member of the San Diego InfraGard chapter for over 15 years and his public sector career includes critical infrastructure protection for water and wastewater systems. In 2016-2018, Mr. Watkins participated in and helped lead a national panel of experts from academia, industry, and government in the creation of curriculum standards for a foundational cybersecurity course using competency-based learning principles for the National CyberWatch Center. In the same period, Mr. Watkins also developed curriculum and teaching materials for two graduate-level and three undergraduate-level cybersecurity courses.

David H. Tobey, Ph.D., is an assistant professor of management at Indiana University, South Bend, and the director of research and assessments at the National CyberWatch Center, an Advanced Technology Education center supported by the National Science Foundation. Dr. Tobey is also founder and CEO of VivoWorks, Inc., an accelerated learning company. Previously, he was a serial entrepreneur whose companies have been listed among Inc Magazine's 500 fastest-growing private companies, set international industry standards for systems configuration and integration, and became publicly-traded companies in the early 1990s. He has also

[31] Ibid.
[32] Smith, Aurelia, 2018.
[33] Hilario, Humberto, 2018.
[34] Stevens, Dwayne, 2018.

served as a consultant, officer and/or board member for private and public companies in the distribution, financial services, hospitality, information technology, life sciences, publishing, and transportation industry sectors.

Casey W. O'Brien is executive director and principal investigator at the National CyberWatch Center in Baltimore, Maryland, an Advanced Technology Education center supported by the National Science Foundation. He is also a professor at Prince George's Community College, and CEO of CaseVero, LLC. Mr. O'Brien has been a director or leader of cyber security and technology groups at various colleges and universities, and participated on national committees related to cyber security, technology innovation, and cyber defense competitions. Mr. O'Brien has been a keynote speaker, and made presentations at many conferences related to education, cyber security, and becoming a NSA/DHS Center of Academic Excellence in Cyber Defense. He has been the technical editor for several textbooks, and authored or co-authored several resource guides and other publications.