Enhancing Cybersecurity Capability in Local Governments through Competency-Based Education

Ronald Pike
Cal Poly Pomona
rpike@cpp.edu

Abstract

Local government agencies face significant challenges related to cybersecurity. Advances in cybersecurity threats have been part of the difficulty, but government agencies, particularly communities, also face unique challenges given their broad mandates and challenges. This is particularly true in large metropolitan areas where activities cross many local and county jurisdictions yet require a coordinated and collaborative response. Local jurisdictions face differing cybersecurity challenges related to local issues such as criminal activity, population, and the mix of land use as well as external considerations such as ports, airports and international borders requiring enhanced coordination with state and federal authorities. Rapid ongoing changes in technology also provide a relentless pattern of change which must be managed. These widely differing challenges, along with resource constraints, lead neighboring communities to possess widely varying cybersecurity capabilities. This research project is an effort to speed the process of training and developing talent to meet these challenges.

1. Introduction

This paper is the result of an ongoing project to enhance cybersecurity capabilities within a major metropolitan region in the United States in preparation for upcoming activities that will stretch the region's ability to meet cybersecurity challenges. While the scope of this research includes SIEM (Security Incident and Event Management) systems, threat hunting, threat intelligence, SCADA, IoT, SDI, SASE and more, the largest challenge by far is the human management of these systems. Managerial control of the cybersecurity resources lies in the hands of more than forty local and regional entities as well as state and federal partners.

Managing cybersecurity operations for a broad set of interconnected technologies across a large region is a difficult challenge. Adding the need to gain consensus and cooperation across a diverse set of regional governments that must all participate in planning and operational control of these systems is much more difficult. The complexity of the problem is vexing for senior leadership and this project is focused on improved training processes to help alleviate challenges. This paper examines enhancing training processes for hands-on cybersecurity operators across the region. This research effort relies upon the NICE (National Initiative for Cybersecurity Education) framework to develop consistent language and skills offering opportunities for leaders to enhance technical consistency and trust relationships across organizational lines.

This project also faces new technology challenges as the organizations are in various states of moving to cloud computing making the current infrastructure fragile as it is spread across multiple technologies and is changing constantly as the deployment process progresses. At the same time, the solution of operating in cloud data centers has proven unacceptable requiring the move to a new edge computing infrastructure while the last movement from traditional computing to cloud computing is still under way.

Proposed solutions to address the training challenges facing the project draw from the NIST NICE framework. The project also draws from the Competency-Based Education (CBE) literature that has been growing for some time and has been identified as useful for academic training related to homeland security as well as digital badging to provide real-time insight into organizational cybersecurity capabilities. Specifically, this paper draws from CBE work in the medical field and offers a definition for CBE in the cybersecurity field with specific relevance to challenges faced by government agencies.

2. Local government challenges

Communities face three critical challenges given they are targeted by attacks, the attacks are increasing and they have limited resources to address the challenges [1]. Furthermore, local governments are typically small and isolated and typically without

URI: https://hdl.handle.net/10125/70860
978-0-9981331-4-0

resources to address cybersecurity challenges, or large and pressed into urban and sub-urban settings where they have a need to work collaboratively with one another despite differing leadership and potentially different values and priorities.

The cybersecurity challenges within local governments are often far more serious than one city having a more talented group of cybersecurity professionals or a better collection of cybersecurity tools and platforms than another. The differences are often more nuanced and have a great deal to do with the challenges or problems a city or other agency faced in the past. So, a highly skilled cybersecurity professional may have skills in one or a few siloed areas within cybersecurity but little or no understanding of other areas.

Also, employment practices within local governments lead to transitioning employees from areas of the organization where work is diminishing to areas that are growing. As a result, leaders are often inheriting employees with related skill sets as opposed to hiring new employees with the desired skill sets. This process of transitioning employees requires that local governments establish effective training processes on the limited resources mentioned earlier. Furthermore, a 2020 study by the U.S. Bureau of Labor Statistics reveals there were 112,300 information security analyst positions open in 2018 and there is expected to be a 32% increase by 2028 [2]. This growth in cybersecurity positions is higher than any other occupation. As a result, local governments would have a difficult struggle to recruit new cybersecurity talent even if they were to have open positions.

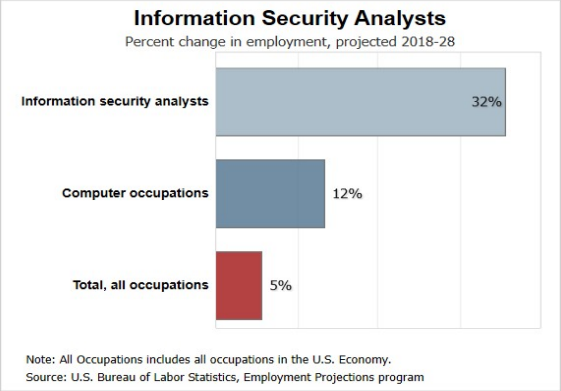

Figure 1: Projected job growth

As cybersecurity challenges are engaged and information is shared between organizations, the information may be shared with individuals who have no related background or limited awareness of the topic. As a result, an individual may take no action, or potentially worse, the individual may take the wrong action in response to shared information. To work seamlessly across many cooperating agencies requires trust which requires a way to ensure consistency of knowledge skills and abilities across the workforce.

3. NIST NICE

Local governments need to coordinate with one another and engage in seamless activities and related training must be aligned with all partner and stakeholder organizations. The NIST (National Institute of Standards and Technology) NICE (National Initiative for Cybersecurity Education) framework was designed to address the type of challenges that the local governments in this study are facing [3]. The NICE framework identifies KSAs (Knowledge Skills and Abilities) needed to unify cybersecurity activities within a workforce.

The NICE framework's KSA's are aligned with cybersecurity standards dealing with issues such as recommended security controls [4] and continuous monitoring [5]. NIST guidance lays out a blueprint for securing systems and the NICE framework provides a structured path to ensure employee training is harmonized with partner agencies as well as federal standards.

The depth and maturity of the NICE framework as well as the many standards to which it is linked is an incalculable advantage to organizations that are growing their cybersecurity capabilities. A seemingly attractive solution to a given problem may tie the organization's hands in future years as their cybersecurity maturity grows and the NICE Framework can serve to mitigate this risk.

Local government agencies have widely varying levels of maturity given their size, focus on cybersecurity and regulatory or other requirements to work with agencies at state or federal levels. As a result, the NICE framework helps organizations with less mature cybersecurity capabilities to recognize downstream requirements and make current decisions that take future requirements into account.

The NICE framework also equips organizations to run criticality and proficiency analyses. These analyses allow organizations to assess which KSA's are most important to their needs and then to determine levels of expertise needed in each of the skills areas to meet cybersecurity goals which in turn provide a skills development roadmap.

4. Competency based education

When it became clear that educating a workforce to manage local cybersecurity infrastructure was the

primary challenge in the project a process was launched to determine the best structure for training. It was already clear from team members' previous experience and regulatory requirements that NIST standards and the NICE framework were going to define much of the training. However, a structural component was needed to ensure 1) that training was focused on needed outcomes, not on educational processes, 2) that training represented the most expeditious path to successful learning, and 3) that learners were the focus of the training and that learners view the training as supportive and helpful rather than tedious and judgmental.

Competency Based Education (CBE) was selected after a review of learning strategies. The process of focusing on learning as opposed to teaching or training was key to moving the selection process away from more traditional teaching/training formats to CBE.

In a book edited by John Burke, CBE is referred to as a quiet revolution in vocational education and training [6]. CBE has its roots in vocational education and has focused on education and training [7]. While there is a great deal of research and exploration around CBE, there is little work focusing on cybersecurity or in IS or IT. Looking for an appropriate reference field in which there has been extensive work in CBE led to the medical field.

There was a call for the use of CBE as a training platform published in the Journal of Homeland Security and Emergency Management that also made a compelling case for CBE to be used in this project [8]. The authors argue homeland security to be a meta-discipline, like medicine and law, including faculty and learning outcomes from other core disciplines.

The medical field was also initially considered as an exemplar in the use of CBE for cybersecurity due to the recommendation by Davenport and Markus for IS to emulate the medical and legal fields [9] with a similar argument to Ramsay and Irmak's argument regarding homeland security. While this paper does not touch on the issue of rigor vs. relevance which was the core of the Davenport and Markus paper, the authors also provided a compelling argument for parallels between IS and medicine/law which this research draws upon.

Both IS and medicine deal with a wide range of technical knowledge requiring significant skills building. Also, both disciplines have an extremely high rate of change in terms of required knowledge and skills given the high degree of development and change in each of the disciplines. IS professionals need to practice their trade to be effective much like a medical practitioner who must run a clinical practice along with their teaching. Davenport and Markus also point out the relevance of literature in the medical and legal fields which allows the literature from these disciplines to be used as learning materials within the disciplines, something that IS has failed to accomplish due to sacrificing relevance for rigor.

4.1 CBE in medical literature

There is a broad set of literature in the medical field arguing for CBE use to train professionals. In 1978, an effort to define CBE in the medical literature conclude "The intended output of a competency-based program is a health professional who can practice medicine at a defined level of proficiency, in accord with local conditions, to meet local needs. It would be pointless to suggest that there is a single definition" [10, p. 18].

Subsequent work in the medical field determined that a definition for CBE is useful even if it relates to core content that does not address local contexts. Such subsequent work includes descriptions of CBE including "an orientation to curricular outcomes in contrast with time-based curriculum", "an organizing paradigm that de-emphasizes process issues in medical training", "an outcomes-based approach to curriculum design and a method to ensure that health professions training is societally responsive" [11, pp. 631, 632].

Medical literature contains tens of thousands of papers on CBE with many useful outcomes but Frank et al. [11] provides a literature review that reveals the common themes. First among the common themes is that "CBE is a distinct approach because of its dedication to predefined graduate abilities as the organizing principle". Frank et al. also notes that medical authors "collectively promoted the concept of progression of competence, meaning that learners advance along a series of defined milestones on their way to the explicit outcome goals or training" [11, p. 633].

Frank et al. [11, p. 636] conclude their pursuit of a definition of CBE in medical education as follows:

> Competency-based education (CBE) is an approach to preparing physicians for practice that is fundamentally oriented to graduate outcome abilities and organized around competencies derived from an analysis of societal and patient needs. It deemphasizes time-based training and promises greater accountability, flexibility, and learner-centeredness.

A draft of a definition of CBE related to cybersecurity in a government context was derived from the organizational needs of local governments collected during this project, the NICE Framework, and the CBE definition of Frank et al. as follows:

> Competency-Based Education (CBE) is an approach to preparing cybersecurity professionals in a manner that is oriented to learner abilities. CBE is organized around competencies based on the

knowledge, skills, abilities, and tasks defined by the NICE framework and specified in NIST SP 800-181. Such competencies are derived from an analysis of societal, organizational and government needs. CBE deemphasizes time-based training and promises greater accountability, flexibility, and learner centeredness.

5. Learning pathways

CBE literature from the medical field called for a learning process that contained defined milestones and a clear goal yet also be learner centered and flexible. There are learning pathways for operators of nuclear power plants and children learning to use an iPad. Earlier and more rigid forms of learning pathways were summarized as a route selected by a learner to build progressive knowledge. A pathway would provide a theory of instruction and guidelines for teachers and curriculum developers [12]. Later definitions of learning relaxed constraints and focused on performance improvement and defines a path as an ideal sequence of learning activities that drive employees to reach proficiency in their jobs. A learning path is viewed as a process not an event and enables learners to find new ways to drive out waste with improved results [13].

Learning paths have been developed for the current project and an example is shown in Figure 2.

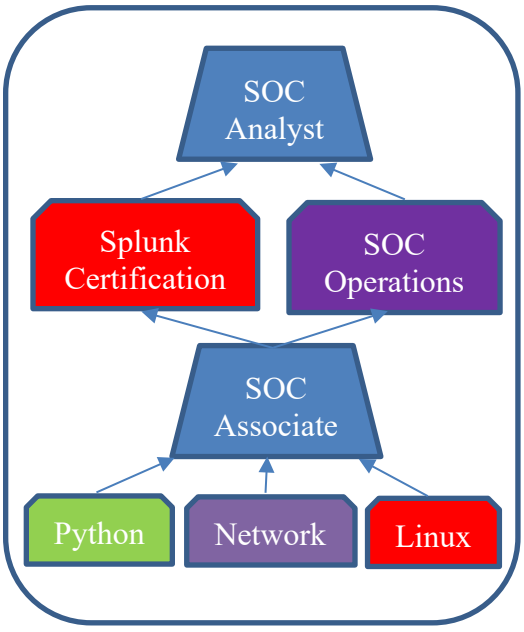

Figure 2: SOC Learning Pathway

Figure 2 shows a pathway for university students in the region of the project to pursue a Security Operations Analyst (SOC) role in the project. The positions available are SOC Associate and SOC Analyst and the learning outcomes required for each position are shown in various colors. An individual represents value to an organization by attaining the SOC Associate position. Value to the organization increases as the individual progresses to the SOC Analyst role The green (Python) outcome refers to a formal course offered through various schools and online. The red items are achieved only through online courses and industry certification. The purple boxes show items that can be attained through formal courses at a nearby college or university or through extra-curricular learning activities at the local university. In each case, students have defined outcomes but multiple opportunities to complete each outcome.

6. Digital badging and e-portfolios

Digital badging and e-portfolios are believed to be important for government employees in this context as support for learners as well as operational support of the program. Literature supported three reasons to include digital badges. First is the potential extrinsic motivation related to earning a badge [14]. Second is the potential for badges to help learners make sense of the learning pathways required to reach a desired goal [15]. Third is the potential to create mechanisms for employers to recognize the fit between potential project team members and open positions [16]. There is some support within the literature for the second and third items (employees understanding pathways to goals and employers understanding the fit between employees and roles) becoming symbiotic and opening constructive dialogues between employees and management to achieve objectives.

The literature also supported three reasons to include e-portfolios which are learner self-reflection, learner storytelling and linking theory to practice. E-portfolios, as a tool for self-reflection, provide the ability to view one's self in completely different ways. Whether a person is trying to understand their current job performance, move from help desk to a deep technical role, or perhaps from a deep technical role to an analytical or managerial role, it is critically important to be able to use self-reflection to support the endeavor [17]. Learner storytelling is needed to help individuals find a voice in the organization. Employees with critical information may sit silently by as they haven't learned to express themselves in their newfound environment and with their newfound terminology and jargon [18], [19]. Linking theory to practice has the most verbose coverage in the literature as it helps learners to contextualize new knowledge and skills and determine how they fit into their work making the new knowledge and skills applicable [20], [21].

Table 1 summarizes the benefits of digital badging and e-portfolios on the development of a local government cybersecurity workforce. While the benefits are not unique to either cybersecurity or local governments, they are particularly useful in this context as management and workers strive to move organizations forward to meet cybersecurity challenges.

Table 1 E-Portfolio and Digital Badging Benefits

Benefits of E-Portfolio and Digital Badging	
E-Portfolio	Digital Badge
Self-reflection	Extrinsic motivation
Storytelling	Illuminate learning pathways
Linking theory to practice	Display employee sufficiency relative to KSA's

6.1 Operationalizing badges and e-portfolios

In past years, the process of offering and managing digital badging and e-portfolios was cumbersome and time-consuming causing organizations to move away from them. It is important to note that industry providers such as LinkedIn, Instructure and Portfolium have reduced the complexity and cost of managing such infrastructures. These vendors also make functionality simple and achievable on mobile devices.

A review of these services and organizations offering training related to cybersecurity also suggests that vendors are already putting infrastructures in place to support the use of badging as a mechanism for organizations to track employment development. Also, while the focus of this study was on cybersecurity training there was clear evidence of many other current uses linking to employee's fitness devices, tracking community service and many other employee-related functions.

6.2 Badging leaderboard

Badging can be leveraged to achieve multiple goals. Two primary goals are certainly to recognize learners' achievements and to illuminate learning pathways helping learners to chart a learning path from where they are to the goals they want to achieve, these attributes of digital badges are shown in the Table 1. The third attribute shown in Table 1 is the ability to display employee sufficiency relative to KSA's.

This third attribute of badging is currently being leveraged in new and exciting ways. Whether the view into badging is a leaderboard or another tracking mechanism it is becoming a uniquely valuable attribute in organizations. This value is based on the ability to enhance organizational outcomes while also more effectively distributing opportunities and managing opportunity equity.

A key component in enhancing organizational outcomes is the open window that badging, coupled with a management interface or leaderboard, provides to display the talents and skills of individuals. Creating teams of people to work on a project or engage a challenge is no longer dependent on just turning to the familiar resources, rather there is an ability to search out the specific skills needed and the people brought into the process may be surprising. This process can expand the number of employees who become core contributors to the organization.

The opportunity equity portion of the value equation is simply the other side of the coin. Employees who are working hard, building new skills and talents, and finding new ways to contribute to the organization can be overlooked as their achievements are not easily visible to managers and leaders. Digital badging and some form of leaderboard or other dashboard allows users to get their achievements and capabilities out in front of management supporting their ambitions to move careers forward.

7. Summary and path forward

Local government agencies face significant challenges managing the current state of cybersecurity needs while also embracing new requirements. The current project requires more than forty cities and related government organizations to work together to meet emerging cybersecurity needs.

The new requirements for cybersecurity readiness include tens of millions of new devices (primarily IoT devices) along with new managerial and control capabilities. Cities and related agencies are understaffed and have been working to move away from locally managed systems to cloud computing while developing cloud computing skills necessary to maintain cybersecurity objectives in the new environment.

However, designs to meet new requirements do not scale adequately with existing cloud computing and communications technologies which is forcing designs toward SASE (Secure Access Service Edge) and edge computing technologies. Many major functions need to

move out of cloud data centers to which they were recently moved and instead be operated in a new edge environment. The new edge environment requires a completely new authentication and encryption scheme that radically shifts the cybersecurity landscape.

This new security footprint often referred to as "security-as-a-service" requires not only the development of new skills but also a completely different contextual framework to make sense of the new operating environment. The rate of change in cybersecurity has always been intensely high but perhaps is higher now than ever as workloads are abstracted away to ever greater extents and the role of a cybersecurity analyst starts to fuse with software developers.

The volume of work and requirement to retrain on frequently emerging new technologies with limited resources requires a new strategy to train new and existing employees getting them prepared as quickly as possible while also providing a feedback mechanism to management with all employees and the current status with badging empowering appropriate decisions on training and work scheduling.

7.1 Cybersecurity apprenticeships

There are no easy answers to meeting the constant increase in cybersecurity challenges coupled with the rapid rise in new technologies requiring constant talent training and development. However, one potential source of help can be found in the German higher education system. For many decades Germany has operated traditional and vocational higher education systems side-by-side. By blending elements of the traditional and vocational systems Germany has been able to grow apprenticeship programs placing large numbers of students into work environments with government and industry partners [22].

An exciting path forward would be the formation of an apprenticeship program that could start between universities that participate in the CAE (Centers for Academic Excellence) program and federal agency partners along with local and regional organizations. Students would complete their final year of school while working near full time for a government agency. The student would receive academic credit for the work they are doing for the agency and take additional courses online to complete their degree requirements.

Such a program would help transition cybersecurity talent to government employment, help to mitigate the cybersecurity labor crisis, and provide students much needed experience. The ability to earn digital badges in cybersecurity while on the job could illuminate learning pathways and enhance student engagement and performance while also potentially augmenting the work experience with measurable skills development and help to meet accreditation requirements linked to credit offered for work experience.

The relatively low number of advanced courses taught online has been a hinderance for such a plan in the past. However, the blight of COVID19 has brought a great many classes online that were never there before. The recent rise of cloud computing, video conferencing and internet bandwidth allowed many courses to be taken online with some new advantages and in some cases a number of disadvantages.

Our school, and likely all others, are searching for good things that can come from the COVID19 tragedy. A cybersecurity apprenticeship program would be a wonderful gift to cybersecurity students, local, state and federal government agencies in need of cybersecurity talent, and the entire nation.

8. References

[1] G. White, K. Harrison, and N. Sjelin, "The Need for Information Sharing and Analysis Organizations to Combat Attacks on States and Communities," in *Proceedingsofthe52ndHawaiiInternationalConferenceonSystemSciences*, HI, USA, pp. 2852–2860, [Online]. Available: http://hdl.handle.net/10125/59722.

[2] "Information Security Analysts: Occupational Outlook Handbook." Bureau of Labor Statistics, Apr. 10, 2020, [Online]. Available: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

[3] W. Newhouse, S. Keith, and G. Witte, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework." National Institute of Standards and Technology, Aug. 2017, [Online]. Available: https://doi.org/10.6028/NIST.SP.800-181.

[4] "Recommended Security Controls for Federal Information Systems and Organizations 140-2, Change Notice April 2014." National Institute of Standards and Technology, 2009, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-53r3.pdf.

[5] "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations." National Institute of Standards and Technology, Sep. 2011, [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-137/final.

[6] J. Burke, *Competency Based Education and Training*. London, New York, Philadelphia: The Falmer Press, 2005.

[7] R. Harris, H. Guthrie, B. R. Hobart, and D. Lundberg, *Competency-based Education: Between a Rock and a Whirlpool*. South Melbourne, Victoria Australia: National Centre for Vocational Education Research, 1995.

[8] J. D. Ramsay and I. Renda-Tanali, "Development of Competency-Based Education Standards for Homeland

Security Academic Programs.," *J. Homel. Secur. Emerg. Manag.*, vol. 15, no. 3, p. N.PAG-N.PAG, Sep. 2018.
[9] T. H. Davenport and M. L. Markus, "RIGOR VS. RELEVANCE REVISITED: RESPONSE TO BENBASAT AND ZMUD.," *MIS Q.*, vol. 23, no. 1, pp. 19–23, Mar. 1999.
[10] W. McGaghie C., G. Miller E., A. Sajid W., and T. Telder V., "Competency-based Curriculum Development in Medical Education." World Health Organization, 1978, [Online]. Available: https://files.eric.ed.gov/fulltext/ED168447.pdf.
[11] J. R. Frank, R. Mungroo, Y. Ahmad, M. Wang, S. De Rossi, and T. Horsley, "Toward a definition of competency-based education in medicine: a systematic review of published definitions.," *Med. Teach.*, vol. 32, no. 8, pp. 631–637, Aug. 2010.
[12] J. Clement, "Model based learning as a key research area for science education," *Int. J. Sci. Educ.*, vol. 22, no. 9, pp. 1041–1053, 2000, doi: 10.1080/095006900416901.
[13] J. Williams and S. Rosenbaum, *Learning Paths Increase Profits by Reducing the Time it Takes Employees to Get Up-To-Speed*. San Francisco: Pfeiffer, 2004.
[14] D. Gibson, N. Ostashewski, K. Flintoff, S. Grant, and E. Knight, "Digital Badges in Education," *Educ. Inf. Technol.*, vol. 20, no. 2, pp. 403–410, Jun. 2015.
[15] C. Pitt R., R. Strickman, and K. Davis, "Supporting learners' STEM-oriented career pathways with digital badges," *Inf. Learn. Sci.*, vol. 120, no. 1, pp. 87–107, 2019.
[16] V. Raish and E. Rimland, "Employer Perceptions of Critical Information Literacy Skills and Digital Badges," *Coll. Res. Libr.*, vol. 77, no. 1, pp. 87–113, 2016.
[17] A. Carl and S. Strydom, "e-Portfolio as Reflection Tool during Teaching Practice: The Interplay between Contextual and Dispositional Variables," *South Afr. J. Educ.*, vol. 37, no. 1, 2017.
[18] I. Rafeldt, H. Bader J., N. Lesnick Czarzasty, E. Freeman, and J. Snayd, "Reflection Builds Twenty-First-Century Professionals," *Peer Rev.*, vol. 16, no. 1.
[19] L. Chin-Yuan and W. Cheng-Chih, "Promoting Nursing Students' Clinical Learning Through a Mobile e-Portfolio," *CIN Comput. Inform. Nurs.*, vol. 34, no. 11, pp. 535–543, 2016.
[20] J. Chittum R., "The Theory-to-Practice ePortfolio: An Assignment to Facilitate Motivation and Higher Order Thinking," *Int. J. EPortfolio*, vol. 8, no. 1, pp. 27–42, 2018.
[21] S. Cunningham, M. Bartesaghi, J. Bowman, and J. Bender, "Re-Writing Interpersonal Communication: A Portfolio-Based Curriculum for Process Pedagogy and Moving Theory into Practice," *Int. J. Teach. Learn. High. Educ.*, vol. 29, no. 2, pp. 381–388, 2017.
[22] M. Baethge and A. Wolter, "The German skill formation model in transition: from dual system of VET to higher education?," *J. Labour Mark. Res.*, vol. 48, pp. 97–112, doi: https://doi.org/10.1007/s12651-015-0181-x.