MAPPING OUT O*NET DATA TO INFORM WORKFORCE READINESS CERTIFICATION PROGRAMS

Micheline Al Harrack

Department of Data Science, Information Technology, and Cybersecurity,
Marymount University, Virginia, USA

ABSTRACT

*The Occupational Information Network O*NET did not explore possible uses of O*NET data to inform workforce readiness certification programs. In this study, the O*NET database is used to map out education requirements and how they relate to professional certifications as required by the employers and job designers in accordance with the National Initiative for Cybersecurity Careers and Studies (NICCS). The search focuses on the "Information Security Analysts" occupation as listed on O*NET, Careeronestop, U.S. Bureau of Labor Statistics (BLS), and finally tied back to NICCS source work role to identify certifications requirements. No site has listed any certification as required, desirable or mandatory. NICCS under the NICE Cybersecurity Framework Work Roles offered general guidance to potential topics and areas of certification. Careeronestop site under certification finder provided the ultimate guidance for this role certification. Professional certifications are still not an integral part of the Cybersecurity Workforce Framework official guidance.*

KEYWORDS

*Occupational Information Network O*NET, NICE Framework, NICCS, Certification & Information Security Analyst.*

1. INTRODUCTION

The Occupational Information Network (O*NET) website was launched in 1998 by the U.S. Department of Labor (DOL). At the heart of this model is a content framework to organize the characteristics of occupational data into what is referred to as hierarchically structured taxonomy comprised of six categories or "domains" [1]. The O*NET model consists of a valuable electronic database containing information designed to help students, educators, job seekers, employers, and workforce trainers and developers, among others. This data collection system organizes job titles into more than 1,102 occupations. However, O*NET did not explore possible uses of O*NET data to inform workforce readiness certification programs. The O*NET database is used in this study to map out education requirements and how they relate to professional certifications as required by the employers and job designers in accordance with the National Initiative for Cybersecurity Careers and Studies NICCS. The search focuses on the "Information Security Analysts" occupation as listed on O*NET with all related job titles, cross-referenced with Information Security Analysts on the U.S. Bureau of Labor Statistics, on Careeronestop, the site sponsored by the Department of Labor (DOL), and mapped back to the NICCS work role titles "All-Source Analyst", and "Information Systems Security Manager". This establishes a simple guide for professionals to align education requirements to potential certifications based on an occupation role for a successful and sustainable career in cybersecurity.

David C. Wyld et al. (Eds): CONEDU, NBIoT, MLCL, ISPR, CSITA - 2021
pp. 119-125, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.110610

2. BACKGROUND AND METHOD

The O*Net foundational framework is based on a content model that integrates the most important component of an occupation broken down into six areas. The worker-oriented attributes are the workers characteristics, requirements, and experience. The job-oriented are the occupational requirements, characteristics, and occupation-specific information (see Figure 1, O*NET content model).

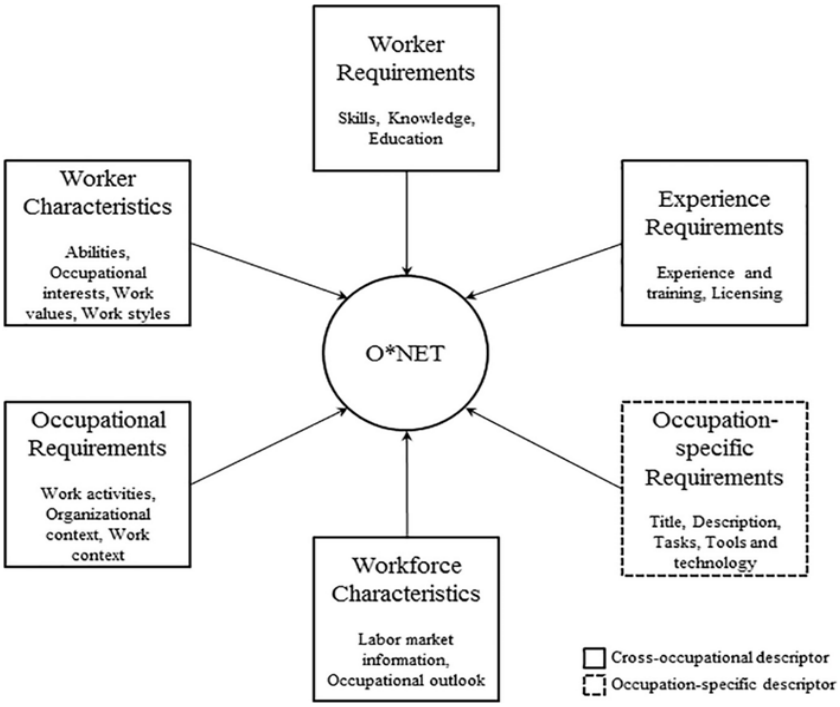

Figure 1. O*NET Content Model [3]

2.1. O*NET Content Model Analysis

Three of these six areas are worker-oriented:
Worker characteristics: Abilities, occupational interests, work values, work styles.
Worker requirements: Skills, knowledge, and education.
Experience requirements: experience and training skills – entry requirements licensing.
The other three are job–oriented:
Occupational requirements: generalized work activities, detailed work activities, organizational context, and work context.
Workforce characteristics: Labor market information, occupational outlook.
Occupation-specific information: tasks, tools, and technology.
Worker characteristics and occupational requirement are cross occupations descriptors while experience requirements and occupation-specific information are occupation specific descriptors as can be inferred [2].

2.2. O*NET Electronic Database

The second instrument in the O*NET model consists of a valuable electronic database containing information designed to help students, educators, job seekers, employers, workforce trainers, and workforce developers, among others. This data collection system organizes job titles into more

than 1,102 occupations. The National Center for O*NET development continually collects data related to these occupations and identifies ways to improve data collection, use, efficacy, and efficiency. With the ever-evolving technology and new job titles, positions, and duties being added constantly to the workplace and workforce, the need to create a standard common description and acknowledged skills, abilities, and other related factors is crucial to stay current and relevant to the users for career and employment guidance as well as workforce development and human resource management. After exploring the site for cyber-related occupations, it appears that O*Net framework does not explicitly list professional certification required or recommended for cybersecurity jobs.

2.3. O*NET Information Security Analyst Work Role Analysis

On the O*NET site, the search is focused on the occupation "Information Security Analyst" to compare with the outcomes of All-Source Analyst, Information Systems Security Developer, and Information Systems Security Manager and draw connections for certificates recommended or required on the NICSS site. The summary report of Information Security Analyst contained a list of activities undertaken by an information security analyst each starting with a specific action verb: "Plan, implement, upgrade, or monitor security measures for the protection of computer networks and information. May ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure. May respond to computer security breaches and viruses" [4]. The Information Security Analyst work role includes a sample of related job titles: Data Security Administrator, Information Security Officer, Information Security Specialist, Information Systems Security Analyst, Information Systems Security Officer, Information Technology Security Analyst (IT Security Analyst), Information Technology Specialist, Network Security Analyst, Security Analyst, Systems Analyst. It lists 12 tasks, 51 technology skills, 8 knowledge areas, 15 related skills, 17 abilities, 21 work activities, 10 detailed work activities, 22 work context criteria. The education lists four-year degree for some jobs but not for all, some job-related skills, knowledge and experience, job training, with job zone examples. 53% of subjects surveyed reportedly hold a bachelor's degree, 23% a post – baccalaureate certification, and 13% an associate degree. The report is available in a detailed fashion with a customized option. The page provides a link to (ISC)2, COMPTIA, ISACA, and National Initiative for Cybersecurity Education (NICE) among others as resources for additional information. O*NET provides a crucial design for employers and human resource professionals to employ job descriptions and selection tools pursuant to Americans with Disabilities Act (ADA) and Equal Employment Opportunity (EEO) requirements [5]. Recruitment officers and human resource personnel employ these detailed descriptions to design job titles, duties, and requirements to attract the needed workforce. Furthermore, the detailed skills, education requirements, experience, and other qualifications provide a framework for standard job description, requirements, and qualifications. An equally important function is to show that the knowledge, skills, abilities, and other characteristics (KSAO) employees need to do their work effectively are related to critical tasks to document the adequacy of hiring and the need for training and workforce development [6]. No certification requirement is listed. Under Credentials, Find Certifications link redirects to Careeronestop.

2.4. U.S Bureau of Labor Statistics: Information Security Analyst

The Bureau of Labor Statistics (BLS) estimates a faster-than-average growth rate in employment of information security analysts, a labor category that represents a significant subset of the cybersecurity workforce. The U.S. Bureau of Labor Statistics in its Occupational Outlook Handbook under Computer and Information Technology, summarizes the job outlook for an Information Security Analyst with quick facts, lists and bachelor's degree as a requirement for most related positions and links back to the O*NET site for additional resources and information

[7]. However, it is noted that, on how to become one, under Licenses, Certifications, and Registrations, BLS states that most employers prefer that employees hold certifications which validate knowledge required for an Information Security Analyst. It distinguishes between more generic certifications such as Certified Information Systems Security Professional (CISSP), and more specific ones like penetration testing and systems auditors specifically.

2.5. National Initiative for Cybersecurity Careers and Studies NICCS: All-Source Analyst

For validation purposes, this work role was searched for on the National Initiative for Cybersecurity Careers and Studies NICCS website under the NICE Cybersecurity Workforce Framework Work Role [8]. The Information Security Analyst is not listed independently rather it has to be searched under All-Source Analyst work role title and any work role ID. This search resulted in the following description: "Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations." [9]. The role description listed 18 abilities, 56 knowledge areas, 18 related skills, and 42 related tasks for all-source analyst. The capabilities indicators were listed by certification/credentials, education, continuous learning, and experiential learning and divided into three categories: entry level, intermediate, and advanced. Education was not essential for entry level with bachelor's as an example. For intermediate level, a bachelor's degree was recommended. For advanced level, a master's or Doctorate degree was recommended. As for certifications, for an entry level they were labeled as not essential but may be beneficial with potential areas covering new attack vectors such cloud computing and mobile platforms. Other areas included vulnerabilities, threats, audit, IT governance and management and information systems related topics without specifying designated commercial certificates. At the intermediate level, a certificate was recommended with topics covering security and risk management, security engineering, communications and network security, software development security, and identity and access management security among very defined security topics. At the advanced level, certifications were deemed not necessary but might be beneficial with focus on project management areas, other topics listed at the entry and intermediate level in addition to specific topics focusing on U.S. privacy laws and practice areas. For this work role, it is obvious that the O*NET framework provides a valid context to generate KSAO and other related job requirements to compile job descriptions, roles, qualifications and attract qualified workforce looking for a common standard in a more increasingly non-conventional world and workplace. However, the guidance is very generic and the language is not authoritative as it relates to certifications. For comparison purposes, the Information Security Systems Manager had education recommended for all three levels starting with a bachelor's degree for the first two up to a Master's and Doctorate for an advanced level. However, certifications ere not essential for entry level but provided an extensive list of potential beneficial areas of certifications. Certificates were recommended for the other two levels with areas of focus identical on the intermediate level to the all-source analyst topics area, and more focused on security, risk, and management areas on the advanced level. The NICCS in its 2020 cybersecurity workforce toolkit stated "Earning certifications enables staff to stay current on in-demand skills and become leaders in the cybersecurity field" [10]. The three certifications listed were COMPTIA+, Certified Information Security Specialist CISSP, and GIAC Security Essentials (GSEC).

2.6. Careeronestop Certification Finder

Using the toolkit on the Careeronestop site and searching for "Information Security Analysts", the results included 116 certifications from 26 providers. These certifications are available by providers in a downloadable excel file. The providers included: Broadcom Inc., Amazon.com

Web Services, Cisco Systems, EC-Council, IBM Corporation, Dell, Oracle, Microsoft, Wireshark, Global Information Assurance Certification, Hewlett Packard Certification and Learning, COMPTIA, International Information Systems Security Certification Consortium, Inc., and several other specific ones. The 116 certifications focused on different areas on information security and topics listed on NICCS site under the NICE Cybersecurity Framework roles for all-source analyst.

2.7. To Certify or not to Certify?

A certification is considered a measurable outcome to assess the knowledge and information acquired within academia and the workplace. Not surprisingly, conceptual knowledge would not replace practical skills and operational excellence for cybersecurity jobs. Recent research shows that holding an IT certification positively influences hiring and job retention, in addition to earning potential. However, two-to-four-year degree holders are less likely to be laid off and potentially earn higher income than non-degree holders [11]. Industry certifications help qualify that individuals possess the knowledge, skills, and abilities for work in the job field as much as one-third of cybersecurity-related jobs require some form of certification [12]. The Bureau of Labor Statistics [13] in its current population survey (CPS) on labor force, employment, and unemployment statistics for persons with or without certifications and licenses reported answers to questions to identify persons with professional certifications and licenses after they were added to the Current Population Survey (CPS) in January 2015. Computer and mathematical occupations of 5,352 were included in the 37,237 professional and related occupations constituting a 12.5% of a population size of 45.3%. Only 5.6% had a certification but no license, 6.9% held a license and 87.5% held neither a certification nor a license. Certificates and certifications are helpful to employers to evaluate the skills and knowledge of applicant especially in small organizations where managers are not well versed in cybersecurity issues [14]. Certifications are not conclusive, but they may be given greater importance as construed as indicators of embodiment of knowledge in a specific area as well as interest and commitment in a field of work. Certifications are often pursued as an addition to an academic degree to highlight an area of interest and expertise. In a workshop conducted by the National Research Council in 2013, some workshop participants expressed that certifications played a crucial role in their careers to establish credibility and competence. Others dissented and pointed out that CISSP certification is a perfect example of an over-glorified certification where highly qualified individuals do not hold it or any other certifications and lamented the hyper-emphasis on certifications which would restrict their employment prospects if required in the candidate selection process. Some participants indicated that some certifications are not viewed positively in some organizations where the experience, the practical skills, the educational attainment, and other factors were better measure and more sought after. They reported omitting certain certifications on their resumes for specific jobs. Views and perceptions on certification differ. While some job seekers, mostly entry and intermediate levels, view certifications as an entry ticket initially and advancement as they pursue career growth, other professionals focus on gaining experience, practical skills, knowledge and furthering their educational goals. Indeed, almost all sites listed educations and degree from Associate to a Doctorate as recommended and beneficial acquisition ability, or educational achievement, were seen as better measures. A few said that they sometimes omitted listing them on their resumes for this reason.

3. CONCLUSIONS AND FUTURE WORK

In analyzing O*NET database for Information Security Analyst for work role certifications, no valuable and actionable information was available. Links to other government sites were listed for additional resources. The Bureau of Labor Statistics listed general guidance while offering an

example of CISSP for general certifications and cited other specific areas like pen testing or systems auditing. NICCS under the NICE Cybersecurity Framework Work Roles similarly offered general guidance as to potential topics and areas of certification for this work role based on the career level: entry, intermediate, and advanced. Finally, Careeronestop site under certification finder was the ultimate guidance for certification tied to the role "Information Security Analyst". Not one site has listed any certification as required, desirable or mandatory. Certifications are still not an integral part of the Cybersecurity Workforce preparation and requirements even as they gain more momentum with job seekers and employers. Current frameworks do not integrate certifications in a prominent manner contrary to the popular belief. In the context of shortage of skilled workforce, the cybersecurity workforce dilemma is more than a solution to a staffing problem; rather it should be a competitive advantage in a proactive agile business model. With private and public sectors competing for the same assets in a time when the pipeline is still lagging in preparing adequately educated and trained cybersecurity professionals, this problem is widespread in academia, business, government, and other types of organizations [15]. Future potential work is possible exploration of adequate workforce preparation mechanisms, and avenues for investing in the human power as it is reported that 71% to 76 % of the businesses are not investing in their long-term assets of "manpower" via training, professional development, and career path development [16] while companies are investing more in infrastructure and advanced technology. The human factor is still trying to grasp the extent of the new landscape complexity. The shortage itself creates a vicious circle as understaffed departments and overworked professionals are led to burnout and eventually turnout.

REFERENCES

[1] National Research Council, 2010. *A Database for a Changing Economy: Review of the Occupational Information Network (O*NET)*. Washington, DC: The National Academies Press. https://doi.org/10.17226/12814 https://www.nap.edu/read/12814/chapter/11

[2] Researchgate.net (n.d.). https://www.researchgate.net/figure/ONET-content-model-21_fig1_317600739

[3] www.onetcenter.org, 2020. *The O*NET Content Model*. Retrieved from https://www.onetcenter.org/content.html

[4] www.onetonline.org, 2020. National Center for O*NET Development, Bureau of Labor Statistics, O*Net Online Summary Report for 15-1122.00—Information Security Analysts. https://www.onetonline.org/link/summary/15-1122.00

[5] SHRM (2020) *Performing Job Analysis.* https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/performingjobanalysis.aspx

[6] Bauer, T., Erdogan, B., Caughlin, D., & Truxillo, D. (2019). *Fundamentals of Human Resource Management*. Sage Publication Inc.

[7] Bureau of Labor Statistics (2020, July 12). U.S. Department of Labor, *Occupational Outlook Handbook*, Information Security Analysts.https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

[8] Newhouse, W., Keith, S., Scribner, B. & Witte, G (2020). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf#page21

[9] National Initiative for Cybersecurity Careers and Studies NICCS, 2020. *NICCS Education and Training Catalog.* https://niccs.us-cert.gov/training/search

[10] NICCS, 2020. https://niccs.us-cert.gov/sites/default/files/documents/pdf/cybersecurity_workforce_development_toolkit.pdf?trackDocs=cybersecurity_workforce_development_toolkit.pdf

[11] Belanich, J. & Morriosn, J. (2019, March). *Impact of Professional Credentials on Employability*. https://www.researchgate.net/publication/334170431. DOI: 10.13140/RG.2.2.20406.96324

[12] Stines, A. (2020, March 24). Faculty Perceptions of Open Educational Resources in Cyber Curriculum: A Pilot Study Curriculum: A Pilot Study. *Beadle Scholar*

[13] Bureau of Labor Statistics (2020, January 21). Labor Force Statistics from the Current Population Survey. https://www.bls.gov/cps/demographics.htm#certs_licenses

[14] National Research Council, 2013. *Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision-Making*. Washington, DC: The National Academies Press. https://doi.org/10.17226/18446

[15] Mailloux, L. & Grimaila, M. (2018, May/June). "Advancing Cybersecurity: The Growing Need for a Cyber-Resiliency Workforce," in *IT Professional*, vol. 20, no. 3, pp. 23-30. doi: 10.1109/MITP.2018.032501745.

[16] Olstik, J., (2019, April). The lives and Times of Cybersecurity Professionals. https://www.esg-global.com/hubfs/pdf/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Apr-2019.pdf

AUTHORS

Micheline Al Harrack has been a Faculty at Marymount University for around six years. Her research interests include Machine Learning Applications, Statistical Analysis, Function Points, Linguistics, and Cyber security topics.

© 2021 By AIRCC Publishing Corporation. This article is published under the Creative Commons Attribution (CC BY) license.