Asian Journal of Multidisciplinary Studies
Vol. 4, No. 2, (2021)
ISSN 2651-6691 (Print)
ISSN 2651-6705 (Online)

A Literature Review of Empirical Studies on Cyber Security Workforce Development

Elmar B. Noche
College of Computing Studies
Pangasinan State University
Pangasinan, Philippines
elmarbnoche_ms@psu.edu.ph

Abstract *– This paper presents an empirical study on the challenges of cybersecurity workforce development. The research paper reflects on the understanding of the different issues and challenges in the earlier years. The literature review demonstrates the identified solutions to the specific challenges and the lapses of the cybersecurity workforce's development, examines current research on the topic, and points out gaps in the existing literature. The study's findings revealed that cybersecurity workforce development encountered issues in the past years, but this has resolved most of the challenges. However, there are still issues that continue in recent years and have yet to be addressed, which affect the development of the cybersecurity workforce development. These problems provide insight for further studies and keep future researchers and cybersecurity workforce development.*

Keywords – Cyber Security, Workforce, Networking, Skills, Employment

1 INTRODUCTION

As digital dangers develop, the online protection labor force's interest arrived at a primary degree of deficiency expected to be at 3.5 million by 2021. [23]. Addressing this demand, cybersecurity workforce improvement ought to have a long-term exertion to fulfill the workforce deficiency of nowadays and prep and get ready the youthful ones to be interested and genuine almost getting into the cybersecurity industry [20].

Cybersecurity encompasses a large variety of job profiles demanding various degrees of technical or non-technical skills. Cybersecurity is now considered an independent discipline following Cabaj et al. [1] or meta-discipline by Parrish [2]. Cybersecurity is "a computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries"— it includes the creation, operation, examination, and testing of secure computer frameworks; and incorporates perspectives of law, approach, human variables, morals, and chance administration [1].

As IoT advances and culprits of cybercrimes extend their instruments and approaches, the request for cyber-professionals develops. Enrollment and work conveyance websites report a deluge of cyber-related work postings [4]. Further, Forbes reports that more than 200,000 cybersecurity employments within the U.S. stay open in 2016, with 1 million work postings worldwide. They also note that the anticipated shortage will reach 1.5 million [6]. As these shortages have become more intense, the weight will be put on the corporate, scholastic, and government pioneers to fill cybersecurity workforce positions with profoundly qualified staff. With such a tall request and short supply of quality cybersecurity laborers, compensation will proceed their upward slant for all disciplines inside the cybersecurity workforce, counting back workforce like frameworks directors and organize engineers. [7]

The hole within the current ponders of the cybersecurity workforce and what skills are

vital for the long run. Characterizing the information, abilities, qualities, and other characteristics that the country needs in its cyber workforce isn't as basic as depicting a gathering of specialized skills that individuals can be prepared for. [29] it should get the different work parts, optimize group organization to suit current and future assignment requests, and how each cyber proficient will fit as a portion of an organization [7].

This paper aims to carry out a systematic literature review of empirical evidence about the different cybersecurity workforce development challenges. This review will focus on answering the following questions:

1) What are the various issues and challenges in identifying individuals and teams' characteristics in the cyber workforce?

2) What are the solutions presented to address the problems and challenges? And

3) What are the factors of these remaining challenges affecting the cybersecurity workforce development selection?

This paper will recognize the issues that affect cybersecurity workforce development by reviewing the existing body of empirical research on the topic.

2. METHODOLOGY

2.1 General database search

The findings of functional studies in this literature review were published studies on different electronic databases such as Google Scholar, Semantic Scholar, Springer, Science Direct, ACM (Association for Computing Machinery), Research Gate, and IEEE (Institute of Electrical and Electronics Engineers). A variety and combination of keywords were used in the review, including *developing the cybersecurity workforce, cybersecurity development, issues and challenges on cybersecurity development, and creating cybersecurity personnel.* Furthermore, after the initial searches in electronic databases, the number of criteria is specified to select relevant studies for inclusion in the review. The paper selection process included 1) empirical study evidence regarding cybersecurity workforce development, 2) published as articles journals, 3) have an abstract, and 4) the research method is demonstrated clearly. A citation was excluded if 1) it was in academic settings such as book review, 2) it was a book or chapter, or 3) no empirical data was reported. The information was systematically collected, including the authors, year of publication, objectives of the study, the settings, the method used (research design, data collection, and analysis techniques), and the main results.

2.2 Identifying the issues and challenges in cybersecurity workforce development.

The researcher got data from different writing sources based on research articles, worldwide reports, current industry happenings, and showcase patterns. After the literature is gathered, the researcher sorts them out to determine the relevance of finalizing the representative literature to the topic. The literature's significance is based on purpose, authority, effectiveness, and reliability.

There are two parts in organizing the process of determining the different difficulties of identifying a cybersecurity workforce. In the first part, the journals are examined against the presence and prohibition criteria. The journals without practical evidence related to the issues and challenges of the cybersecurity workforce development are eliminated in the review. The remaining journals that have potential are obtained to be analyzed further in the next part. In the second part, the reviewed journals' challenges are listed, and the overview of each issue is summarized.

2.3 Recognizing the solutions for the issues and challenges in cybersecurity workforce development.

Added investigation of the problems listed and challenges are done. The researcher further analyzed the solutions in every issue and challenge in identifying the cybersecurity workforce. Several solutions have been identified for the challenges. However, these solutions did

not resolve all the problems in identifying the cybersecurity workforce. In this part, all of the identified challenges and their corresponding answers are separated into two parts; 1) challenges that already have a solution, and 2) remained challenges that anticipate the resolution. The additional searches through references are also conducted in this part, where the researcher further investigated the connections of the initially found papers and the references made to those papers. The supplementary investigation is used to validate if the cybersecurity workforce development still has no solution to the identified remaining challenges in recent years.

2.4 Identifying the factors of those remaining challenges affecting cybersecurity workforce development.

Qualified peer-reviewed research papers related to the remaining cybersecurity workforce development issues were left for review. In this part, the articles were examined to determine the factors affecting the cybersecurity workforce development concerning the issues that remained.

3. RESULTS AND DISCUSSION

3.1 General database search

Table 1 shows the number of papers in each of the databases that were identified using the key search. The second column in table 1 contains all the results, including the non-scientific writings such as magazine articles. In all, there are 74 journals examined against the inclusion and exclusion criteria. Based on the reading of abstracts, 38 journals are excluded from the review, and the remaining 36 journals with potential are acquired. The remaining full texts journal articles are evaluated to check if it has empirical evidence. Finally, 12 articles are excluded, and 24 qualified peer-reviewed research papers on cybersecurity workforce development were left for review.

Table 1. Results from searched databases.

Database	Total number of result	Peer review paper
IEEE	1059	3
Springer	936	5
Semantic Scholar	4830	7
Research Gate	189	5
ACM	25	1
Science Direct	370	3
Google Scholar	14,900	n/a

3.2 Issues and challenges in identifying cybersecurity workforce development.

The ever-growing demand for cyber-enabled systems and services has made cybersecurity one of the most severe challenges we face in the 21st century. [1 Logan O. Mailloux] As stated by Hoffman et al. [16] recognized the importance of building a multidisciplinary cybersecurity workforce. Bagchi-Sen et al. [4] identified a gap between purely technical Training geared towards early career professionals and the interpersonal, communication and business-oriented skills required to progress in the field. Cyber administrators with more encounters (particularly those working in intrigue groups) are superior able to get the KSAs (e.g., "delicate" abilities) vital to illuminate complex cyber-issues. [10] However, cybersecurity may be an unused teach; in this way, teaches are not fundamentally experienced in extending real-world issues or have not had formal preparation on errand examinations or directions plan, supporting the course and educational modules improvement. [7]

Most of the reviewed papers reported common cybersecurity workforce development problems in their study. Through analysis, eight challenges are identified that cybersecurity workforce development encountered in recent years.

Challenges	**Paper**
User Awareness	[16][18][7][6]

Higher Education	[16][1][2]
Training	[16][18][1]
Integrated Education Systems	[16][3][7]
Collaboration Government, Industry and Academia	[16][2]
Certification	[16][18][7][1]
Skills	[16][18][7][1]
Cyber Training	[16][1]

Table 2. Challenges for Cybersecurity Workforce Development.

Cybersecurity workforce development's challenges are user awareness, higher education, Training, integration into the education system, collaboration training between government, industry, academia, certification, and budget. As supported by on UK NCSS [19], the national methodology for cybersecurity workforce advancement challenges are with client mindfulness, cybersecurity higher instruction, preparation, integration into the instruction framework, the collaboration between industry, government, and the scholarly world, certification, allotment of budget, aptitudes counseling, cyber preparing center and career and preparing the way. [21]

Client mindfulness is the biggest challenge within the cybersecurity workforce advancement, as emphasized in each NCSS analyzed. [13] Cybersecurity could also be a collective duty and requires adding up to exertion for each partner to reinforce add up to defense on the internet, which collective responsibility does not work due to differences and that reinforcement for security is lacking. [17] Training and certification are profoundly empowered within the current workforce community, but only a few practices encompass the cybersecurity workforce. [11] Also, up-skilling and reskilling for mid-career experts are too focused on drawing modern participants into the calling. Still, the concern is the budget for upskilling and reskilling are not well funded. Based on research, only a few certifications are the road to secure and certify the professional skillset based on universally recognized benchmarks. [10] Finally, collaboration with the industry and the scholarly community is incapable of exchanging industry needs and information into the academic community to get the understudies ready to meet industry desires. [12]

3.3 Identified solutions for the issues and challenges in cybersecurity workforce development.

There have been a lot of studies concerning the different problems and challenges in cybersecurity workforce development. Table 3 shows the identified solutions in the challenges of cybersecurity workforce development.

Solutions	Paper
Communication between Different Stakeholders	[16][18][23][20][1]
SMART Goals	[23][20][16][12]
Cybersecurity Workforce Database	[23][20][12]

3.3.1 Communication between Different Stakeholders

For the cybersecurity workforce improvement methodology to be compelling, the partners require constant communications. [23]. Teoh and Mahmmod [20] highlighted that the government, industry, the scholarly world, and instruction framework got to match up with the cybersecurity ability prerequisites, requests, availabilities, and potential. Furthermore, these partners should incorporate creating the cybersecurity workforce national methodology to supply inputs and commitments. This will guarantee the demand and supply of the ability pool within the country are in line.[23]

3.3.2 SMART Goals

The SMART is Specific, Measurable, Achievable, Realistic, and Timely goals.[16] SMART has a timeline, and nitty-gritty activity arranges with the partners' characterized parts and duties, counting the lead organizations. In this way, it will increase the accountability and

commitment of the stakeholders.[12] Furthermore, the victory estimation will be a checking tool to guarantee that the country is on track towards the cybersecurity workforce objective.

3.3.3 Cybersecurity Workforce Database

Human assets with abilities and involvement in cybersecurity are too included within the cybersecurity workforce database. This will give a list of accessible abilities.[23] Also, it'll ease Preparing, mentoring, and preparing of the cybersecurity workforce. Furthermore, the database can too be utilized as a career way of arranging and aptitudes admonitory. It will avoid the loss of cybersecurity talent.[23][20]

3.4 Recognizing the factors that remain challenges affecting cybersecurity workforce development.

A further review was conducted and found out that one of the significant factors that affect creating a cybersecurity workforce is employment challenges.

3.4.1 Employment challenges

Challenges are surrounding developing and maintaining a robust cybersecurity workforce within the national security community. Across the Atlantic, a U.S. report [28] reiterated similar challenges seen in the Federal Cybersecurity Workforce, namely: 1) demand outstripping supply for cybersecurity professionals, 2) skills gap in cybersecurity positions, and 3) agency strategic workforce plans that do not specifically address cybersecurity workforce needs [19] Compounding the challenges faced by the cybersecurity skills shortage are those of enticing and retaining the information security experts needed within the National Security space and public sector space more broadly.[30]

3.4.2 Payscale issues

A 2015 report by the U.S. Department of Justice highlighted the FBI's struggle in attracting computer science recruits, mainly due to low pay [21]. The FBI, responding to the report, said "the cyber workforce challenge runs through the federal government" and that it was necessary to develop "aggressive and innovative recruitment and retention strategies" [21].

The public service, facing competition challenges from the private sector in recruitment and personnel retention, will need to innovate and respond in a much more agile way to market forces to attract and keep the best cyber personnel.[23] Furthermore, given the challenges in competing on remuneration, organizations that offer additional benefits on the job; such as ongoing training and professional development, a clear career path within the cybersecurity field, ongoing engagement with outside stakeholders, vendors, and academia, to inform their employees' cybersecurity expertise, will likely have a stronger case for retaining their cybersecurity professionals.[20]

The summary of the analysis shows the current solutions for the cybersecurity workforce and the remaining issues. By presenting the factors of the remaining challenges affecting cybersecurity workforce development, it will now uncover the factors why these challenges persisted in recent years.

4. CONCLUSION

In this paper, a discussion of the cybersecurity workforce development research is done. Specifically, the researcher (a) reviewed the different issues and challenges in implementing a cybersecurity workforce development; (b) discussed the identified solutions for the specific problem and addressed the remaining challenges; and (c) addressed the factors affecting the development of the cybersecurity workforce.

In this paper, the researcher figures out the challenges in cybersecurity workforce development, namely user awareness, education, training, collaboration government, industry and academia, Certification, and Skills. These problems can be further exacerbated by the changing nature of the technology on which cybersecurity workforce development is implemented.

Most cybersecurity workforce development challenges have already been solved using Communication between Different Stakeholders, SMART Goals, and Cybersecurity Workforce Database. Some of the identified solutions resolve numerous cybersecurity workforce development challenges because most of the challenges are relevant and somewhat connected. For instance, Numerous government initiatives are in place to address the cyber skills shortage and legislation that will provide the means for the public service to become more competitive in attracting and retaining the best and brightest individuals. In a few cases, countries actualize National Cyber Security Techniques (NCSS) to address cybersecurity issues and give a national-level vital exertion to flourish on the internet. The typical accentuation of the NCSS analyzed are basic framework security, cybercrime assurance, cybersecurity proficient improvement, cybersecurity open mindfulness, investigate and improvement (R&D), and universal collaborations. However, to address this issue, cybersecurity workforce development is a long-term effort. It involves initiatives to groom and prepare the young ones in school to be interested and serious about getting into the cybersecurity industry. The analysis suggests that these issues are continuously developing due to the rapid technological changes, so there is no absolute solution for these challenges.

Another fundamental problem considered in this study was the remaining issues of Employment challenges for cybersecurity workforce development. The factors affecting employment have a low salary, and the level of experience is rare. Moreover, consideration for the appropriate technical and analytical rigor is essential to ensure that cybersecurity workforce solutions are feasible to key stakeholders.

5. FUTURE WORK

Several more questions are relevant to the cybersecurity workforce development and its issues and challenges beyond this research's scope due to time constraints. It is suggested to conduct more study about how cybersecurity workforce development, how employment and payscale issue will be addressed and the other matrics to filter a right candidate on developing cybersecurity workforce.

6. REFERENCES

[1] Cabaj, K., Domingos, D., Kotulski, Z., and Resp´ıcio, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. Computers & Security, 75, 24–35.

[2] Parrish, A., Impagliazzo, J., Raj, R.K., Santos, H., Asghar, M.R., Jøsang, A., Pereira, T., and Stavrou, E. (2018). Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. In Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education, 36–54. ACM.

[3] Campbell, S.G., ORourke, P., and Bunting, M.F. (2015). Identifying dimensions of cyber aptitude: the design of the cyber aptitude and talent assessment. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, volume 59, 721–725. SAGE Publications Sage CA: Los Angeles, CA.

[4] A. Freeman. (2016, July 15, 2016). Could we see an influx of cybersecurity job roles in 2016? Available:https://www.technojobs.co.uk /info/tech-news/20160105-couldwe-see-an-influx-of-cyber-security-job-roles-in-2016.phtml

[5] Army Cyber Branch Annex (2017). Army DA PAM 600-3Cyber Branch. Available at: https://www.armystudyguide.com/content/publications/da_pams/da-pam-6003.shtml [accessed April 15, 2018].

[6] S. Morgan. (2016) One Million Cybersecurity Job Openings in 2016. Forbes. Available: http://www.forbes.com/sites/stevemorgan/2016/01/02/onemillion-cybersecurity-job-openings-in-2016/#7a235147d274

[7] Caulkins, B. D., Badillo-Urquiola, K., Bockelman, P., and Leis, R. (2016). "Cyber workforce development using a behavioral cybersecurity paradigm," in Proceedings of the International Conference for Cyber Conflict U.S., eds C. Connelly, A. Brantly, R. Thomson, N. Vanatta, P. Maxwell, and D. Thomson (West Point, NY: Army Cyber Institute). DOI:10.1109/CYCONUS.2016.7836614

[8] R.M. Ryan, and E.L. Deci, "Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being," American psychologist, 55(1), 2015, pp. 68-78.

[9] Sobiesk, E., Blair, J., Conti, G., Lanham, M., & Taylor, H. (2015). "Cyber education: a multi-level, multi-discipline approach," In Proc. of the ACM 16th Annual Conference on Information Technology Education, 43-44.

[10] Cybersecurity, C. o. E. N. (2016). Report on Securing and Growing the Digital Economy. NIST.

[11] Elkhannoubi, H., & Belaissaoui, M. (2015). Fundamental Pillars for an Effective Cybersecurity Strategy. Paper Presented at the Computer Systems and Applications (AICCSA).

[12] Fourie, L., Pang, S., Kingston, T., Hettema, H., Sarrafzadeh, H., & Watters, P. (2014). The Global Cyber Security Workforce: An Ongoing Human Capital Crisis. Paper presented at the Global Business and Technology Association Conference.

[13] ISACA. (2017). State of Cyber Security 2017: Part 2: ISACA.

[14] Haber, E. & Kandogan, E. (2014). "Security administrators: a breed apart," In Workshop on Usable I.T. Security Management (USM'07) held with the ACM Symposium on Usable Privacy and Security: SOUPS '07.

[15] Hawkey, K., Botta, D., Werlinger, R., Muldner, K., Gagné, A., & Beznosov, K. (2015). "Human, organizational, and technological factors of I.T. Security," In CHI '08 Ext. Abstracts on Human Factors in Computing Systems, 3639- 3644.

[16] Hoffman, L., Burley, D., & Toregas, C. (Mar 2016). "Holistically building the cybersecurity workforce," IEEE Security & Privacy, 10(2), 33-39.

[17] ISC2. (2017). 2017 Global Information Security Workforce Stduy: ISC2.

[18] Huang, H., Kvasny, L., Joshi, K. D., Trauth, E. M., & Mahar, J. (2017). "Synthesizing I.T. job skills identified in academic studies, practitioner publications and job ads," In Proc. of the SIGMIS Conference on Comp. Personnel Research, 121-128.

[19] U.K.Government. (2016). National Cyber Security Strategy 2016-2021.

[20] Teoh, C. S., & Mahmood, A. K. (2017). National Cyber Security Strategies for Digital Economy. Paper presented at the Research and Innovation in Information Systems(ICRIIS).

[21] U.S., D. (2015). The Department of Defense Cyber Strategy

[22] Markus, M. L. & Benjamin, R. I. (Dec 1996). "Change agentry – the next I.S. frontier," MIS Quarterly 20(4), 385- 407.

[23] Teoh, C. S., & Mahmood, A. K. (2017). Cybersecurity Workforce Development for Digital Economy. The Educational Reviewing, USA, (1), 136-146.

[24] J. Davidson, " 'Inadvertent' cyber breach hits 44,000 FDIC customers," vol. 2016, ed. Washington Post online: Washington Post, 2016.

[25] A. Freeman. (2016, July 15, 2016). Could we see an influx of cybersecurity job roles in 2016? Available:https://www.technojobs.co.uk /info/tech-news/20160105-couldwe- see-an-influx-of-cyber-security-job-roles-in-2016.phtml

[26] S. Morgan. (2016) One Million Cybersecurity Job Openings in 2016. Forbes. Available: http://www.forbes.com/sites/stevemorgan/2016/01/02/onemillion- cybersecurity-job-openings-in-2016/#7a235147d274

[27] Noll, C. L. & Wilkins, M. (2015). "Critical skills of I.S. professionals: A model for curriculum development," Journal of Information Technology Education, 1(3), 143-154

[28] NICCS, "Most Common Degree Programs Associated with Cybersecurity Careers," ed. Washington, D.C., 2016.

[29] Jessica Dawson and Robert Thomson (2018) The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance Front. Psychol., 12 June 2018 | https://doi.org/10.3389/fpsyg.2018.00744

[30] Mulligan, C., Cybersecurity: cornerstone of the digital economy, in Imperial College Business School London. 2017, Imperial College London: London.

[31] Rogers, E. (2003). Diffusion of Innovations (5th ed.), New York, NY: Simon and Schuster.

[33] SANS Technology Institute. "Information Security Master's Degrees: MSISM." Retrieved May 19, 2017, from https://www.sans.edu/academics/masters-programs/msism

[32] Republic, C., National Cyber Security Strategy of the Czech Republic (2015-2020). 2015.

[34] Tham, I., 5 key proposals from Singapore's new Cyber Security Bill, in The Straits Times. 2017: Singapore.

[35] PWC, Luxembourg to become a Cyber Security hub. 2016.

[36] Suby, M. and F. Dickson, The 2015 (ISC)2Global Information Security Workforce Study. 2015, ISC2.

[37] Shafqat, N. and A. Masood, Comparative Analysis of Various National Cyber Security Strategies. International Journal of Computer Science and Information Security, 2016. 14(1): p. 129-146.

[38] Baker, M. (2016). Striving for Effective Cyber Workforce Development. Pittsburgh, PA: Software Engineering Institute.

[39] Champion, M., Jariwala, S., Ward, P., and Cooke, N. J. (2014). "Using cognitive task analysis to investigate the contribution of informational education to developing cyber security expertise," in Proceedings of the Human Factors and Ergonomics Society Annual Meeting, Vol. 58, Philadelphia, PA, 310–314.

[40] Winston, E. R. (Oct 1999). "I.S. consultants and the change agent role,"

ACM SIGCPR Comp. Personnel, 20(4), 55-74.

6. AUTHORS

Elmar B. Noche, MITc
College of Computing Studies
Pangasinan State University
Dagupan City Philippines