ABSTRACT

Malaysia has set a target to achieve a contribution of 22.6% of its Gross Domestic Product (GDP) through the digital economy by 2030. However, cyber-attacks such as online scams are posing a threat to the country's Critical National Information Infrastructure (CNII) and impacting businesses, governments, and individuals. The COVID-19 pandemic has also caused an increase in cybercrime, emphasising the need for cyber resilience. Malaysian government has launched the Malaysia Cybersecurity Strategy 2020-2024 and aims to develop 20,000 cybersecurity professionals by 2025 to address the issue, but currently the country is short on talent due to a skills gap. Therefore, this study aims to identify the demand of Technical and Vocational Education and Training (TVET) cybersecurity workforce by determining the technical competencies, new skills, and job positions required by the industry and evaluating the training institution readiness, as well as discover the best governance practices related to collaboration between government and industry. This study was conducted in four phases, beginning with the preparation of questionnaire, followed by industry engagement, survey consultation, international benchmarking and comparative study of workforce supply and demand. More than 400 companies and 12 training institutions, including DSD Accredited Centre, public universities and private universities were involved in this study. The supply and institution readiness analysis covered respondents from training institutions accredited by the Ministry of Human Resources and the Ministry of Higher Education. Data obtained from the survey were analysed using a statistical method to evaluate the current industry scenario, forecast the workforce's demand for the next three years, and evaluate the quality of the human capital produced by the training institutions. The study discovered that the number of recent cybersecurity related graduates are still insufficient to cater the industry demand for the next three years. Additional training programmes with the professional certificates are required to produce competent workforce, with the majority of job opportunities in the cybersecurity field being in the Information and Communication, and Banking and Finance Sectors. Employers in the CNII sectors are generally satisfied with workers who have a Professional Certificate background, followed by those with degrees. However, employee with experience and skills are given a greater priority. The study forecasts a significant increase in demand for cybersecurity personnel, from 2,460 in 2023 to 11,032 in 2026, with a total required cybersecurity workforce of 24,883 by 2026. To achieve this target, an average of 3,677 workers per year will be required from 2023 to 2026. Training institution also expressed the crucial shortage of certified cybersecurity instructors. In addition, the study found that community participation in cybersecurity is influenced by several factors, including awareness, education, security requirement, government and industry support, career paths and attractive salaries. The study concludes with recommendations to address the undersupply of workforce, improve community participation, financial support and training programmes.