Journal of Applied Economic Sciences
Volume XX, Summer, Issue 2(88), 2025

Cybersecurity Job Requirements in Asian Countries: An Analysis of Workforce Trends and Future Implications

Florian GERTH
https://orcid.org/0000-0002-4809-9789
Asian Institute of Management, Makati, Philippines
Centre for the Study of Global Economic Future (CSGEF), UAE
fgerth@aim.edu

Albert W. K. TAN
https://orcid.org/0000-0001-9678-5882
Asian Institute of Management, Makati, Philippines
atan@aim.edu

Philip T. H. KWA
https://orcid.org/0009-0003-0617-5071
Asian Institute of Management, Makati, Philippines
pkwa@aim.edu

Olivier P. ROCHE
Asian Institute of Management, Makati, Philippines
oroche@aim.edu

Article's history:

Received 4th of May, 2025; *Received in revised form* 19th of May, 2025; *Accepted* of 29th of May, 2025; *Available online*: 22nd of June, 2025. *Published* as article in the Volume XX, Summer, Issue 2(88), 2025.

Suggested citation:

Gerth, F., Tan, A. W. K., Kwa, P. T. H. & Roche, O. P. (2025). Cybersecurity Job Requirements in Asian countries: An analysis of workforce trends and future implications. *Journal of Applied Economic Sciences*, Volume XX, Summer, 2(88), 192-206. https://doi.org/10.57017/jaes.v20.2(88).02

Abstract:

This study maps the evolving cybersecurity talent landscape in four Asian economies - the Philippines, Singapore, Thailand, and Hong Kong - using 223 LinkedIn job postings (August 2024) and mixed quantitative - qualitative analyses. Regression results confirm that senior positions demand, on average, 5.3 years more experience than analyst roles and that Philippine postings require 1.5 years less experience than their Hong Kong benchmark, reflecting country-specific maturity levels of the digital sector. Thematic analysis highlights rising demand for cloud-security, incident-response, and governance skills. Importantly, we link these workforce trends to macroeconomic outcomes: Asia-Pacific now holds 60 % of the global cybersecurity talent gap and closing it could lift developing-country GDP per capita by 1.5 % within a decade. Policymakers therefore face a dual imperative - protecting the digital economy and unlocking productivity gains - by investing in skills pipelines and cross-border talent mobility. Findings inform targeted recruitment, training, and economic-development strategies across the region.

Keywords: cybersecurity, workforce trends, economic impact, Asia, skills requirements, digital economy.

JEL Classification: J23; J24; J44; J62; O33.

Introduction

The field of cybersecurity is constantly evolving, and the demand for skilled professionals is on the rise in Southeast Asia. To bridge the gap between industry needs and the workforce, it is crucial to understand the skills and competencies that are in high demand within the cybersecurity sector. This research aims to identify and analyse the key skills and competencies sought after by employers in the field of cybersecurity. This research employs a mixed-methods approach as shown below by collecting data from LinkedIn and other job portals who are hiring cybersecurity professional to identify current trends, requirements, and expectations of cybersecurity professionals. The research questions for this study are:

Q1: What are the key cybersecurity job titles, and what skills and competencies are most commonly required across different experience levels (entry, mid, and senior) in the current job market?

Q2: What emerging skills and technologies are shaping the future of cybersecurity roles based on recent trends in job postings?

To understand the required skills and traits for cybersecurity jobs, the authors examined hundreds of job postings advertised on LinkedIn during August 2024. We focus on the Southeast Asian region to maximize reliability as well as coverage, and to focus on locations that experience a high demand for data protection and cyber defence, the countries chosen were the Philippines, Singapore, Thailand, and Hongkong.

1. Literature Review

Global integration has paved the way for cross-border industries to harness locational advantages that emerging and re-emerging nations offer. Companies engaged in international business can produce where factors of production, conditional of productivity levels, are most affordable. This is observed more so as growth in demand for traded services outpaces the growth in demand for goods (Lund et al., 2019). While the current trend in globalization can be commonly characterized by its breakthroughs in information technology, emergence of new and advancing economies, increased role of the government, and the deepening of global value chains, a number of scholars have observed that the shifts in high- and low-skilled labour is likewise a manifestation and a growing concern (Das & Hilgenstock, 2022). It is forecasted that about 50% of the labour force would have to reskill and upskill to remain relevant (Li, 2022). These are direct results of globalization efforts and internationally disruptive events. The recent COVID-19 pandemic for instance, impacted where, what, and how people performed daily operational tasks. Jesuthasan, et al. (2020) posits that these events have not only changed the skill set required to succeed; but also, redefined jobs themselves. Today work can be assigned to anyone with the most appropriate skills and availability within the organization, and automation has improved the reliability and safety of performing routine tasks. Even more so, the era of Industry 4.0 has further radically changed the job market - creating new jobs and demanding new skills (Li, 2022).

One of the fundamental and existential disciplines that emerged as technology began to revolutionize how individuals carry out tasks is cybersecurity. As Krzysztof et al. (2018) argue, jobs within this area have become one of the most in demand and most lucrative careers to enter in as it transitioned from a necessity to combat rising criminal attacks on electronic systems, to its own field of study. This seems coherent; as more organizations shifted to digital platforms to run marketing, human resource management, operational, and financial transactions, so did the threat of substantial losses over stolen data. In the Philippines, these losses are estimated to be Php6.5 billion per day. Companies operating in the energy sector, banks, telecommunications, and healthcare are among the most vulnerable to these risks (Crismundo, 2023). With the development of quantum computing, it is more critical now for all actors seeking to enter this trade and for managers operating in these at-risk sectors, to understand the skill set requirement in order to make effective and informed decisions. Over the years, cybersecurity has been studied in three major areas: skills, training, and education (Nkongolo et al., 2023).

Skills

Industry 4.0 not only has increased an organization's dependence on technology, but fast-paced computational advances, even more, lead to multiplier effects and thus the need to skill up (Roser, 2023). This reached the point where cybersecurity - which has evolved with the use of technology, has now become one of the most important concerns among interdependent organizations; alongside sustainability (Sulich et al., 2021). It is unsurprising that data privacy, systems monitoring, and other related skills have grown in demand. Nkongolo et al. (2023) studied these and other requirements necessary to build a career as a cybersecurity professional. Using a systematic literature review approach, the authors screened through 1,520 studies and constructed a list of key technical and soft skills. Chief among these were knowledge of vendor product, troubleshooting, ability to work independently, and teamwork. While this study likewise identifies skill requirements, it reviewed secondary data - journal articles and conference proceedings, to arrive at its conclusion. The primary data for job postings from Asian countries with the highest and least demand for cybersecurity professionals. These have revealed new insights about what skills are required across three categories.

A similar study using systematic literature review, was previously conducted in 2021 by a team of researchers from the Norwegian University of Science and Technology. With the same goal of identifying competencies and skills required in cybersecurity, the authors posited that there was a need to investigate articles focused on critical infrastructure (CI). This effectively allowed an understanding of sector and role-specific requirements to secure organizations that are most at-risk of cyber-attacks and would suffer the highest losses in revenue (Chowdhury & Gkioulos, 2021). Sifting through 28,100 research papers published after the year 2020, the authors discovered that there is no universally accepted skill set and competencies in CI. However, general trends were observed, leading to the construction of a skills mapping table bearing four categories: technical, soft, implementation, and management skills. While these results bear resemblance to this study's criteria for analysis (i.e., technical, soft, and business skills), it does not explore other considerations that employers look at (e.g., age, mindset, personality, recognition, etc.). This additional avenue has allowed the authors to establish not just the skill set required to start a cybersecurity career; but also, the personae preferred by organizations around Asia.

Training

Evidence of a clear high demand and shortage of cybersecurity experts can be observed around the world. To bridge this gap, numerous organizations have adopted ways to upskill their personnel to uphold mandated roles and obligations (Furnell, 2021). These findings are supported by a number of articles, hence the interest in understanding how to best train individuals inside the organization. Glas et al. (2023) contend that training and upgrading the skills of potential experts is critical to overcome the global shortage. Their study examined the use of visual programming languages (VPLs) to learn code-based skills. Using a Randomized Controlled Trial (RCT) in an experimental research design, the authors tested 30 individuals on achievement of learning outcomes, engagement and interest in the training, as well as learning speed. The results showed that learning outcomes were the same regardless of the method deployed; however, participants were observed to have been more engaged in the learning process.

Further research on training effectiveness likewise looked at technology as the practical tool of choice. In 2023, Shojaifar and Fricker evaluated how a self-paced tool could improve the cybersecurity capability of small and medium-sized enterprises (SME) in Switzerland. Through interviews with nine CEO's and CISO's (i.e. chief information security officer), the authors deduced that effectiveness differed across businesses and was not a solution to all SME's (Shojaifar & Fricker, 2023). The results of these studies have revealed that the type and mode of training provided do not have significant impacts on the quality of learning. This paper thus offers a different perspective into the type of actual training expected of cybersecurity experts entering the job market.

Education

While training focuses on upskilling internal applicants to and current employees with cybersecurity roles, education generally concentrates on doing the same for individuals outside an organization. Beyond traditional ways of learning a new skill (i.e., in school), many alternative learning options such as online courses, certificate courses, etc. are now available (Marquardson & Ahmed, 2020). Research in cybersecurity education analysed these options. As observed, the COVID-19 pandemic forced organizations to migrate to digital platforms in order to comply with the remote working setup. This transition caught most businesses off guard and exposed them to considerable risk. Giddeon Angafor et al. (2023) argued that scenario-based exercises such as case studies or simulations, could have improved the situation and facilitate faster recovery from these types of incidents. Their findings point that these types of learning techniques in education, raise cybersecurity awareness. These have allowed individuals to effectively evaluate incident response procedures and improved decision-making.

The same conclusions were drawn by Zhong et al. (2024) when her team examined Reddit users and their perspective on cybersecurity competitions. Using computational text mining and qualitative content analysis to understand the respondents' perceptions, her team discovered that these events not only encouraged novices to upskill; but also, motivated learners to develop a strategic mindset. Coincidentally, while training appears to flock towards technology as a tool, education appears to move more towards the method of teaching (e.g., scenario-based exercises or cybersecurity competitions). This study likewise provides an overview of what alternative skill development programs are acceptable or even expected (e.g., preferred education experience, recognitions, awards, etc.).

2. Research Methodology

This section showcases the data collection process, some descriptive statistics resulting from the data obtained, and the regression model used to obtain statistically robust findings.

To understand the required skills and traits for cybersecurity jobs, the authors examined hundreds of job postings advertised on LinkedIn during August 2024. To remain relevant in the Southeast Asian region, to maximize reliability as well as coverage, and to focus on locations that experience a high demand for data protection and cyber defence, the countries chosen were the Philippines, Singapore, Thailand, and Hongkong. Type of data extracted from LinkedIn are shown in Table 1. After data cleaning, the sample comprises 223 observations.

Table 1: Type of data extracted from LinkedIn

Job Title	The specific title of the cybersecurity job
Company Information	Name of the hiring company, Company size and industry, if available.
Job Description	A detailed description of the responsibilities and duties associated with the position. Specific projects or tasks that the candidate will be involved in.
Skills and Competencies	A list of technical and soft skills mentioned as requirements or preferences. Identify both hard skills (e.g., programming languages, security tools, etc.) and soft skills (e.g., communication, teamwork, etc.).
Experience Level	Minimum and preferred years of experience. Level of expertise (e.g., entry-level, mid-level, senior).
Education Requirements	Minimum educational qualifications (e.g., bachelor's degree, certifications, etc.).
Certifications	Any specific certifications mentioned as requirements or preferences.
Location	The geographic location of the job.
Type of Employment	Full-time, part-time, contract, or other employment arrangements.
Salary Information	If available, extract salary or salary range information.
Application Deadline	If specified, the deadline for submitting applications.

Job Title	The specific title of the cybersecurity job
Contact Information	Information on how to apply (website, email, etc.).
Benefits	Any mentioned benefits associated with the position (healthcare, retirement plans, etc.).
Keywords and Key Phrases	Extract keywords and phrases used in the job description to identify trends and commonalities.
Technology Stack	Specific technologies or tools mentioned in the job description.
Company Culture and Values	Any information about the company's culture, values, or mission mentioned in the job posting.
Language Requirements	If specific language requirements are mentioned.
Travel Requirements	If the position involves travel, specify the extent and frequency.
Application Process	Information on how candidates are expected to apply (e.g., online application, email submission, etc.).

Descriptive Statistics

Figure 1 shows that country composition of the sample. As is shown, the Philippines is the country with the highest number of job advertisements during the sampling period with 78 observations (35%). Singapore follows with 70 (31.4%), then Hongkong with 39 (17.5%), and Thailand with 36 observations (16.1%). Job levels can be summarized into the following categories: Analyst, Supervisor, Manager, and Senior Manager. Figure 2 shows their within-sample distribution. The job level with the highest occurrence is Analyst with 146 occurrences (65.5%), followed by Manager with 37 (16.6%), Supervisor with 31 (13.9%), and Senior Manager with 9 (4%) observations.

Figure 1: Job postings from each country

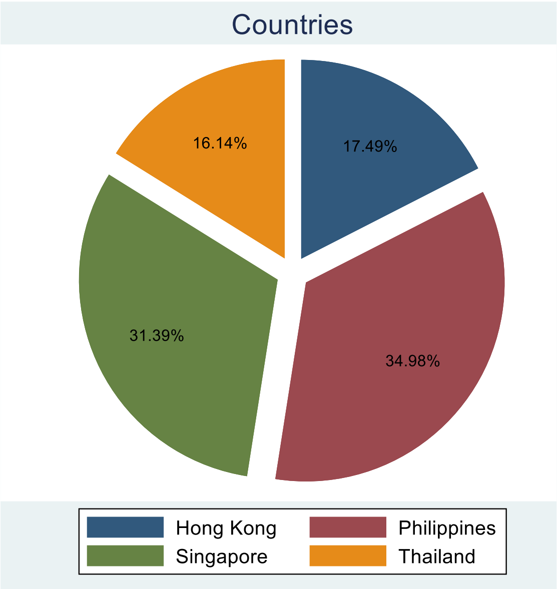


Figure 2: Job levels for cybersecurity

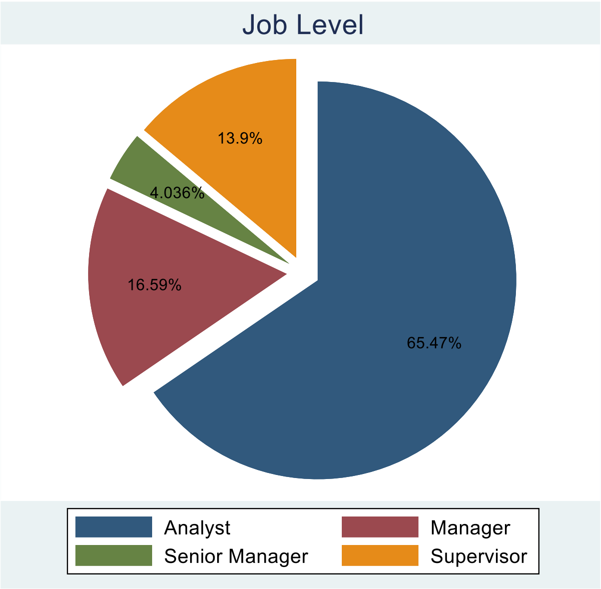
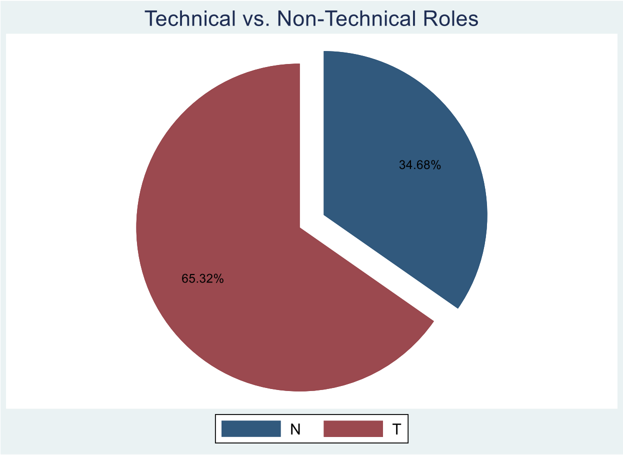


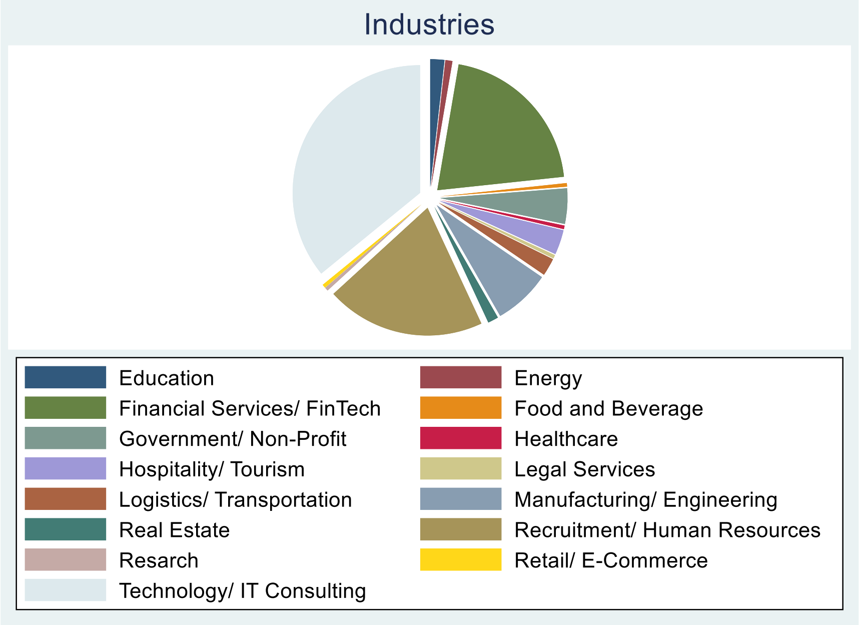
Figure 3 shows the amount of job advertisements that offers technical compared to non-technical roles. Out of the total, 145 (65.3%) are technical roles, and 77 (34.7%) are non-technical roles.

Figure 3: Technical versus Non-Technical Roles



Since data protection and cyber defence are industry are relevant and existential issues spanning across several industries, Figure 4 shows the allocation of industries searching for cyber security personnel. All in all, 15 industries have been identified: education, energy, financial services (including FinTech), food and beverage, government/non-profit, healthcare, hospitality/tourism, legal services, logistics/transportation, manufacturing/engineering, real estate, recruitment/human resources, research, retail/e-commerce, and technology/ IT consulting. The results show that five industries dominated the job market: Technology/ IT Consulting with 80 (35.9%), Financial Services (including FinTech) with 46 (20.6%), Recruitment/ Human Resource with 45 (20.2%), Manufacturing/ Engineering with 16 (7.2%), and Government/ Non-Profit with 10 observations (4.5%).

Figure 4: Industry represented from respondents



To better understand the labour market dynamics and the profile of in-demand roles in the cybersecurity sector within Southeast Asia, a detailed analysis of the job postings was conducted, focusing on three key parameters: years of experience required (Table 2), job offer type and geographical distribution (Table 3), and the most frequently advertised job titles (Table 4).

Table 2 provides insight into the minimum number of years of experience required for posted cybersecurity roles. The data clearly reveals a strong inclination towards early-career professionals. Notably, 22.5% of the job advertisements require zero years of experience, indicating an openness to fresh graduates or newly trained professionals. An additional 18.2% of jobs request two years of experience, while 16.6% request three years, collectively demonstrating that approximately 65% of the total job postings are targeting individuals with three or fewer years of experience. This aligns with the earlier visual analysis presented in Figure 2 and confirms the hypothesis that the cybersecurity job market in Southeast Asia is largely entry-level driven. Only a small fraction of jobs (less than 10%) requires eight or more years of experience, reflecting limited demand for highly seasoned professionals compared to junior or intermediate-level talent.

Table 2: Years of experience expected for the job posted

Years of experiences	Number of observations	Percentage
0	42	22.5%
0.5	2	1.1%
1	11	5.9%
2	34	18.2%
3	31	16.6%
4	7	3.8%
5	28	15%
6	4	2.1%
7	6	3.2%
8	8	4.3%
10	11	5.9%
15	1	0.5%

Table 3 expands the analysis by categorizing job offers according to contract type and geographical location. Full-time roles dominate the landscape, accounting for 128 out of the 223 listings (approximately 57.4%), followed by contract positions at 62 (27.8%). Internships, while less common at 21 postings, still suggest an effort to cultivate new talent. Notably, the Philippines and Singapore emerge as key hubs for cybersecurity hiring. The Philippines leads in job postings with 78 positions, largely full-time and contract roles, suggesting a vibrant but cost-sensitive labour market. Singapore, close behind with 70 job offers, shows a balanced mix of full-time and contract opportunities and demonstrates the country's status as a mature digital economy with ongoing cybersecurity needs. Hong Kong and Thailand follow with 39 and 36 listings respectively, indicating relatively smaller but still active markets. The preference for full-time and contract positions over part-time or internship roles reflects employers' desire for sustained commitment and continuity in critical security functions.

Table 3: Job categories

	Full Time	Part Time	Contract	Internship	TOTAL
Singapore	25	2	27	16	70
Philippines	45	6	26	1	78
Hongkong	25	3	7	4	39
Thailand	33	1	2	0	36
TOTAL	128	12	62	21	223

Table 4 further breaks down the top ten job titles advertised on the platform. The most frequently occurring role is "Senior Analyst, Cyber Security," appearing five times, indicating high demand for analytical roles that blend technical acumen with strategic oversight. Other frequently advertised roles include “Cyber Security Specialist” and “Head of MIS,” each appearing four times, showing the need for both technical implementation and managerial oversight. Several positions such as “Cyber Security Consultant,” “Cyber Security Engineer,” “Security Analyst,” and “Senior Security Consultant” appear three times each, illustrating a relatively even spread across different cybersecurity functions, from consulting and engineering to awareness training and incident response. These roles highlight the diverse nature of cybersecurity demands, ranging from technical execution to strategic leadership.

Table 4: Top ten job titles

Job Titles	Frequency
Cyber Security Consultant	3
Cyber Security Forensic & Incident Response Officer	3
Cyber Security Engineer	3
Security Analyst	3
Support, IT Security Awareness	3
Senior Security Consultant	3
IT Security Specialist	3
Cyber Security Specialist	4
Head of MIS	4
Senior Analyst, Cyber Security	5

Collectively, the data from these tables offers a comprehensive view of the current hiring landscape in Southeast Asia’s cybersecurity job market. It highlights the growing demand for early-career professionals, the dominance of full-time and contractual employment formats, and the concentration of opportunities in key regional economies like the Philippines and Singapore. Furthermore, the job titles advertised reflect a need for both technical skills and strategic capabilities, reinforcing the evolving complexity of cyber defence in a digitally interconnected environment.

3.2 Regression Analysis

An open question remains whether the above variables are statistically relevant in explaining the required minimum number of years of previous experience, see discussion above. To do so, the regression model in Equation (1) is used.

$$Years\ of\ Experience_i = \beta_0 + \sum_{r=1}^{3} \beta_r * IV_{r,i} + \beta_4 * Country + \varepsilon_i \tag{1}$$

where: the dependent variable is the minimum number of years of experience for each individual job advertisement *i (i=1,…,187)*. The independent variables, *IV*, are the three categories from 3 different perspectives namely: job level, technical vs. non-technical role, and industry. The dummy variable *Country* is first estimated on its own, and in subsequent steps maintained as a control variable[1].

[1] Regarding the variable Country, “Hongkong” is the benchmark. Hence, all coefficient values for the variable Country need to be compared to this location. For the variable Job Level, the benchmark is “Analyst”, for Technical vs. Non-Technical it is “non-technical”, and for the variable Industry the benchmark is “Education”. Each is done to avoid perfect multicollinearity between the independent variables ultimately resulting in biasedness and inconsistency.

For comparison purposes and ease of reproducing our results, we use ordinary least squares (OLS) to model Equation (1). We apply adequate care during the estimation process to ensure we comply with the classical linear regression function assumptions. Consequently, the statistical behaviour of the residual terms and the parameter values were analysed, and where necessary, adopted. Furthermore, to prevent misleading diagnostic tests, we calculated the variance as an exponential function of the covariates specified in the model. The last step is necessary because OLS explicitly assumes that the residuals of the variables are constant, which does not apply to our data. Concerning the stability of our results, we use the method-of-moments estimation technique as a robustness test. We obtain the same qualitative and quantitative results by assuming predeterminedness and imposing the moment condition of non-stochastic covariates[2].

Table 5: Regression Results

Variables	Model			
	1	2	3	4
Country				
Benchmark (Hongkong)				
Philippines	-1.47	-0.94	-1.31	-1.52
	(0.58)**	(0.51)*	(0.57)**	(0.012)**
Singapore	-0.72	-0.46	-0.59	-1
	(-0.25)	(-0.53)	(0.62)	(0.63)
Job Level				
Benchmark (Analyst)				
Manager		2.72		
		(0.66)***		
Senior Manager		5.3		
		(0.85)***		
Supervisor		1.52		
		(0.55)***		
Technical vs. NT				
Benchmark (NT)				
Technical			0.79	
			(0.42)*	
Industry				
Benchmark (Education)				
Energy				-1.11
				(1.65)
Financial Services				-0.69
				(1.27)
Food and Beverages				-2.61
				(1.22)**
Government				0.73

[2] For a more detailed analysis and the general applicability of this methodology, see Gerth et al. (2021a, b) and Gerth (2024).

Variables	Model			
	1	2	3	4
				(1.61)
Healthcare				6.87
				(1.21)***
Hospitality				-1.54
				(1.35)
Legal Services				3.87
				(1.21)***
Logistics				0.71
				(1.42)
Manufacturing				1.38
				(1.41)
Real Estate				-0.29
				(1.81)
Human Resources				0.44
				(1.28)
Research				2.39
				(1.22)*
Technology/ IT Consulting				0.13
				(1.23)

Note: Values in brackets below the coefficient values represent their respective standard errors. ***Significant at 1% significance level. **Significant at a 5% significance level. *Significant at a 10% significance level.

With the help of Equation (1), we are proposing four different regression models. Model (1) regresses years of experience on the countries within our data set only. Model (2) includes the variable Job Levels as additional independent information. Model (3) conditions whether the job add is for technical or non-technical roles. Finally, Model (4) takes all different industries into account while estimating the parameters.

Considering Model (1), we see that job advertisements for cybersecurity professionals in the Philippines require around 1.5 years less experience compared to all other countries (not considering job level, technical vs. non-technical roles, and industry). Once we control for the job level, Model (2), the Philippine discount in experience shrinks to around 0.9 years compared to all other countries. However, it still exists. Regarding job level and the years of required experience, Senior Managers need the highest amount of previous experience compared to Analysts (5.3 years), after Managers with 2.7 years, and Supervisors with 1.5 years. All these findings are highly statistically significant at a 99% significance level.

Considering Model (3), when controlling for the role (technical vs. non-technical), the discount in professional experience for the Philippines remains significant and amounts to 1.3 years. Technical roles, on the other hand, require an experience premium of around 0.8 years.

Model (4) shows the same statistical relationship between the experience discount of the Philippines compared to the other countries; around 1.5 years less experience required. In terms of industry requirements, the Food and Beverage industry, compared to the educational sector, asks for an experience discount of 2.6 years. The Healthcare and Legal sectors, on the other hand, require a substantial experience premium of 6.9 and 3.87 years, respectively. Cybersecurity professionals working in the Research sector, are required to have around 2.4 years more experience compared to the educational sector. All other sectors, Energy, Financial Services (surprisingly), Government, Hospitality, Logistics, Manufacturing, Real Estate, Human Resources, and Technology/ IT Consulting, do neither require less nor more years of experience compared to educational sector. Furthermore, Model (4) reconfirms substantive differences among the four economies. Philippine adverts require 1.52 fewer years of experience than Hong Kong ($p < 0.05$), while Singapore's requirement is statistically indistinguishable from Hong Kong. Thailand's point estimate is directionally lower but not significant. These gaps signal distinct stages of cybersecurity-market maturity and have implications for wage levels, outsourcing flows, and cross-border workforce mobility, explored in next section.

3.3 Thematic Analysis

A thematic analysis was conducted to examine the experience requirements and role responsibilities across cybersecurity-related job descriptions. Several key themes emerged from the analysis, reflecting the complexity and breadth of skills demanded in the cybersecurity field.

One of the central themes identified was Cybersecurity and Risk Management. Many roles emphasized in-depth knowledge of information security domains such as incident response, malware analysis, vulnerability assessment, and penetration testing. There was also a strong emphasis on risk management, particularly in OT/IT environments within critical infrastructure. Responsibilities often included designing and implementing security architectures and ensuring compliance through continuous security monitoring.

A second major theme involved Technical Proficiency in Cybersecurity Tools and Systems. Required experience frequently included the use of SIEM technologies, firewalls, endpoint detection and response (EDR) systems, proxy servers, AWS security configurations, and CyberArk. Employers also sought candidates with expertise in infrastructure security, network security, identity and access management, and cloud environments, particularly AWS.

Security Operations and Incident Management also featured prominently. Many roles required experience in operating within Security Operations Centers (SOCs), with an emphasis on managing incidents, performing real-time responses, and handling IT operations. Leadership in incident response was a distinct sub-theme, with several job descriptions requiring candidates capable of managing teams under pressure and conducting simulation exercises to test preparedness. Another important area was Information technology auditing and compliance. Roles often involved conducting IT and security audits, evaluating infrastructure for vulnerabilities, and ensuring compliance with industry frameworks and regulations such as HiTrust. There was also a focus on IT governance responsibilities, such as managing security standards, account lifecycles, and vendor risks.

The analysis further revealed the importance of Leadership and Training. Candidates were expected to lead security teams, coordinate with government or cross-functional units, and provide training on incident response. Effective communication skills were also noted as essential, particularly for translating complex cybersecurity concepts to diverse stakeholders. A separate theme addressed specialized roles and certifications. Job descriptions frequently required certifications such as CISSP, CEH, and CompTIA Security+. Roles included Security Consultants, Cybersecurity Architects, and OT/IT Security Specialists, often focusing on application security, security design, and malware analysis.

In terms of business and industry focus, some roles were specifically tailored to sectors like consulting, legal, and energy. For instance, candidates in the power industry were expected to handle OT security and manage critical infrastructure risks, while those in the legal sector focused on IT governance within corporate environments. Additionally, experience in Helpdesk and Technical Support was commonly mentioned. Roles included IT support, service desk management, and incident troubleshooting, functions fundamental to maintaining operational continuity.

Thematic analysis also extended to roles and responsibilities, where Risk Management and Threat Identification emerged as a core area. Candidates were expected to identify and manage cyber threats using tools such as SIEM and to understand governance, risk, and compliance (GRC) frameworks.

Another key area was Network and Cloud Security, with many roles requiring skills in securing networks, performing penetration testing, and managing cloud environments. Incident Management and Response was again emphasized, particularly in real-time monitoring and forensic analysis.

Under Audit and Compliance, job descriptions stressed the importance of conducting regular cybersecurity audits, ensuring compliance with relevant standards, and assessing risks associated with IT environments.

Client and Stakeholder Engagement was also frequently mentioned, requiring strong communication skills to explain technical issues, consult on cybersecurity strategies, and align security posture with business goals. This theme linked directly to another important area, Sales and Business Development in cybersecurity, highlighting the importance of understanding products, identifying new business opportunities, and managing client relationships.

Project and Operational Management was identified as a recurring theme, especially in roles that involved overseeing cybersecurity projects, ensuring adherence to security protocols, and maintaining comprehensive documentation and reporting structures.

Moreover, a clear emphasis was placed on proficiency in technical tools and frameworks, including penetration testing tools, vulnerability scanners, audit software, and secure coding practices. Familiarity with standards such as ISO 27001, GDPR, and HIPAA was highlighted under the theme of Compliance and Regulatory Knowledge. Both the thematic and regression analyses revealed the critical importance of prior work experience. Regression analysis quantitatively demonstrated how experience requirements vary by job level, role, and industry. For instance, senior managers typically require an average of 5.3 more years of experience than analysts. Thematic analysis supports this by detailing the advanced expertise expected in senior roles, such as leadership in incident response or cross-functional coordination.

Finally, both analyses also aligned in recognizing industry-specific variations. Regression findings indicated that sectors like healthcare and legal demand significantly more experience than education. Thematic insights elaborated on this by identifying sector-specific skills, such as critical infrastructure security for energy sectors or IT governance expertise in consulting and legal firms.

3. Implications of Cybersecurity Workforce Trends in Asia: Economic and Managerial Perspectives

In terms of economic implications of cybersecurity workforce trends in Asia, digital-economy growth in Asia is accelerating, but its sustainability hinges on an adequately skilled cybersecurity workforce. Three macro-level channels are particularly salient.

First, cybersecurity contributes directly to productivity and GDP growth. According to the World Bank, reducing the frequency and impact of cyber incidents in emerging economies could raise per capita GDP by up to 1.5% over a decade by minimizing system downtime, enhancing trust in digital transactions, and facilitating the uptake of higher-value digital services (Cobos, 2024).

Second, cybersecurity strengthens labour market dynamism and inclusivity. As noted in the Asian Development Bank's 2025 Digitalization Policy Report, secure digital ecosystems can help reduce income inequality by expanding access to online employment and services, thus fostering inclusive economic participation across the Asia-Pacific region (ADB, 2025).

Third, the cybersecurity talent gap affects the investment climate and increases operational risk. The 2024 ISC2 Workforce Study reports that Asia-Pacific faces the largest regional shortfall in cybersecurity talent, approximately 4.8 million professionals. Alarmingly, 37% of organizations in the region reduced cybersecurity budgets in 2024, increasing exposure to breaches and creating barriers to foreign direct investment (FDI). Supporting this, a BCG analysis estimates that 60% of the global cybersecurity talent shortage is concentrated in Asia-Pacific, particularly affecting sectors critical to regional exports: finance, manufacturing, and technology (BCG, 2024).

Country-level analyses further illustrate these dynamics. For example, the Philippines, with a low barrier to entry and a strong BPO sector, has emerged as a hub for entry-level cybersecurity talent. However, wage-driven attrition remains a challenge. Conversely, Singapore, with its high GDP per capita. demands advanced skills in leadership and compliance, reflecting its mature digital economy. Hong Kong's finance-centric landscape sustains the highest experience benchmarks, while Thailand is actively scaling through public–private reskilling programs. To ensure regional resilience, policymakers must align education, immigration, and employment strategies with these diverging national profiles.

From a managerial standpoint, the findings offer actionable insights for organizations seeking to attract, develop, and retain cybersecurity talent. Organizations must refine their job descriptions to reflect the distinct experience levels and competencies required for various cybersecurity roles. Senior-level positions, such as incident response leads or compliance managers, demand advanced skills in leadership, cross-functional coordination, and specialized technical domains. Job advertisements should also be tailored to reflect industry-specific requirements, such as OT/IT security in critical infrastructure or regulatory compliance in healthcare and legal services.

In today's dynamic threat environment, cybersecurity professionals must possess not only technical proficiency in tools like SIEM, EDR, and cloud platforms but also leadership and communication abilities. Organizations should prioritize candidates who are capable of leading teams, managing cross-functional initiatives, and translating complex cybersecurity issues for non-technical stakeholders (Cabaj et al., 2018). The fast-evolving nature of cyber threats necessitates ongoing training. Employers should support professional certification programs, such as CISSP, CEH, and CompTIA Security+—as these are frequently cited prerequisites. Additionally, organizations should provide pathways for employees to gain expertise in emerging areas such as advanced threat detection, cloud security, and malware analysis (Chen et al., 2024). Given the regulatory complexity of sectors like healthcare, energy, and finance, hiring strategies should emphasize industry-relevant experience. Familiarity with sector-specific regulations (e.g., HIPAA, GDPR, NERC CIP) is essential to ensure compliance and manage cyber risks effectively.

Cybersecurity is no longer a siloed function; it must be integrated with broader business objectives. The thematic analysis reveals that professionals are increasingly required to engage with clients and stakeholders. Cross-departmental collaboration is important to aligning cybersecurity measures with the organization's strategic goals. As cybersecurity threats become more complex, strategic succession planning becomes essential. Organizations must identify high-potential talent and provide structured development opportunities that prepare individuals for senior technical and managerial roles.

Multinational organizations operating across Asia should optimize human resource deployment by aligning workforce strategies with local conditions. For example, analyst-level SOC operations may be cost-effectively based in the Philippines, while governance or leadership roles may be better suited to high-complexity markets like Singapore. Given the economic impact of cybersecurity labour shortages, industry leaders should collaborate with governments to co-invest in workforce development. Initiatives might include scholarship programs, technical and vocational education and training (TVET), and the creation of mutual-recognition frameworks for certifications to facilitate cross-border labour mobility.

Conclusion

Our evidence confirms that cybersecurity talent shortages are not merely an organizational risk but a macroeconomic constraint: closing Asia-Pacific's skills gap could unlock multi-percentage, point GDP gains while safeguarding digital trade. Country comparisons highlight heterogeneous pathways - from Singapore's high-skill, high-wage enclave to the Philippines' volume-oriented talent pools - offering nuanced levers for policymakers and hiring managers alike. Future work should quantify the elasticity between workforce investment and sector-specific productivity across Asian economies.

First, in response to the question of key cybersecurity job titles and the skills and competencies required across different experience levels, the analysis reveals that senior-level roles, such as Senior Managers, demand significantly more experience (5.3 years) compared to entry-level positions like Analysts. Key competencies across all experience levels include technical expertise in tools and systems, incident response, risk management, compliance, and leadership abilities. Additionally, industries such as healthcare and legal services exhibit higher experience premiums, emphasizing the need for sector-specific knowledge.

Second, emerging skills and technologies shaping the future of cybersecurity roles are identified through both the regression and thematic analyses. The findings underscore the increasing importance of technical expertise, particularly in risk management and advanced cybersecurity tools, which are expected to be pivotal in future roles. Furthermore, the growing emphasis on leadership and cross-functional coordination, particularly in senior positions, signals the evolving nature of the profession, where strategic and operational expertise are as critical as technical capabilities.

Together, these findings highlight the dynamic interplay between technical and non-technical competencies, experience, and industry-specific needs in shaping the cybersecurity workforce. Organizations and policymakers can use these insights to refine recruitment strategies and develop targeted education and training programs, ensuring the cybersecurity workforce is equipped with the necessary skills to tackle emerging challenges.

While this study provides insights into the experience requirements and evolving skills in the cybersecurity workforce, several limitations should be acknowledged, and there are opportunities for further research.

One limitation of this study is the reliance on job postings as the primary data source. Although job postings offer a comprehensive snapshot of current demand, they may not fully capture the evolving nature of skills that are yet to be formally recognized in the industry. Additionally, the study focuses on specific sectors, and findings may not be generalizable to all industries or regions. Furthermore, while the regression and thematic analyses highlight key trends, they do not account for the complex interplay of personal characteristics, such as soft skills and work culture fit, which can also play a significant role in recruitment.

Future research could expand on these findings by exploring the impact of emerging technologies such as artificial intelligence, machine learning, and blockchain on cybersecurity roles. Studies could also delve into the effectiveness of different educational pathways (e.g., certifications versus formal degrees) in preparing candidates for these roles, examining how these credentials align with industry needs. Additionally, longitudinal studies tracking career progression in cybersecurity could provide deeper insights into how experience, skills, and industry trends evolve over time. Finally, examining the global landscape and comparing cybersecurity experience requirements across countries could offer a broader understanding of regional differences and trends.

Credit Authorship Contribution Statement

Gerth, F, Tan, A.W.T, Kwa, P. T. H. and Roche, O. P. contributed equally to the conception and design of the research. Gerth and Tan were primarily responsible for data collection, analysis, and visualization. Kwa contributed to the interpretation of results and literature contextualization. Roche provided guidance on the methodological framework and overall project supervision.

Conflict of Interest Statement

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Angafor, G., Yevseyeva, I., & Maglaras, L. (2023). Scenario-based incident response training: Lessons learnt from conducting an experiential learning virtual incident response tabletop exercise. Retrieved from https://www.emerald.com/insight/content/doi/10.1108/ICS-05-2022-0085/full/html

Asian Development Bank. (2025). Digitalization can reduce persistent inequality in Asia and the Pacific. Retrieved from https://www.adb.org/news/digitalization-can-reduce-persistent-inequality-asia-and-pacific

BCG. (2024). 2024 Cybersecurity Workforce Report: Bridging the workforce shortage and skills gap. https://gcforum.org/en/research-publications/cybersecurity-workforce-report-bridging-the-workforce-shortage-and-skills-gap/

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. Retrieved from https://doi.org/10.1016/j.cose.2018.01.015

Chowdhury, N., & Gkioulos, V. (2021). Key competencies for critical infrastructure cybersecurity: A systematic literature review. Retrieved from https://doi.org/10.1108/ICS-07-2020-0121

Cobos, E. V. (2024). Cybersecurity economics for emerging markets. https://hdl.handle.net/10986/42130

Crismundo, K. (2023). Top listed firms may lose P6.15 billion to cyber-attacks. https://www.pna.gov.ph/articles/ 1202979

Das, M., & Hilgenstock, B. (2022). The exposure to routinization: Labour market implications for developed and developing economies. https://doi.org/10.1016/j.strueco.2021.10.013

Furnell, S. (2021). The cybersecurity workforce and skills. Retrieved from https://doi.org/10.1016/j.cose.2020.102080

Gerth, F. (2024). Nexus Between Financial Inclusion and Economic Activity: A Study About Traditional and Non-Traditional Financial Service Indicators Determining Financial Outreach. In: Muschert, G.W., Pereira, V., Ramiah, V., Cansin Doker, A. (eds) Financial Inclusion. Sustainable Development Goals Series. Springer, Cham. https://doi.org/10.1007/978-3-031-68803-4_20

Gerth, F., Ramiah, V., Toufaily, E. et al. (2021). Assessing the effectiveness of Covid-19 financial product innovations in supporting financially distressed firms and households in the UAE. *Journal of Financial Services Marketing*, 26, 215–225. https://doi.org/10.1057/s41264-021-00098-w

Gerth, F., Lopez, K., Reddy, K., Ramiah, V., Wallace, D., Muschert, G., Frino, A., & Jooste, L. (2021). The Behavioural Aspects of Financial Literacy. *Journal of Risk and Financial Management*, *14*(9), 395. https://doi.org/10.3390/jrfm14090395

Glas, M., Vielberth, M., Reittinger, T., Böhm, F., & Pernul, G. (2023). Improving cybersecurity skill development through visual programming. Retrieved from https://www.emerald.com/insight/content/doi/10.1108/ICS-11-2022-0170/full/html

Jesuthasan, R., Malcolm, T., & Cantrell, S. (2020, April 22). How the coronavirus crisis is redefining jobs. Retrieved from https://hbr.org/2020/04/how-the-coronavirus-crisis-is-redefining-jobs

Li, L. (2022, July 13). Reskilling and upskilling the future-ready workforce for Industry 4.0 and beyond. Retrieved from https://doi.org/10.1007/s10796-022-10308-y

Lund, S., Manyika, J., Woetzel, L., Bughin, J., Krishnan, M., Seong, J., & Muir, M. (2019). Globalization in transition: The future of trade and value chains. Retrieved from https://www.mckinsey.com/featured-insights/innovation-and-growth/globalization-in-transition-the-future-of-trade-and-value-chains

Marquardson, J., & Ahmed, E. (2020, February). Skills, certifications, or degrees: What companies demand for entry-level cybersecurity jobs. Retrieved from https://eric.ed.gov/?id=EJ1246234

Nkongolo Wa Nkonglo, M., Mennega, N., & Zyl, I. (2023). Cybersecurity career requirements: A literature review. https://www.researchgate.net/publication/371684501_Cybersecurity_Career_Requirements_A_Literature_ Review

Roser, M. (2023). This timeline charts the fast pace of tech transformation across centuries. Retrieved from https://www.weforum.org/agenda/2023/02/this-timeline-charts-the-fast-pace-of-tech-transformation-across-centuries/

Shojaifar, A., & Fricker, S. (2023). Design and evaluation of a self-paced cybersecurity tool. Retrieved from https://www.emerald.com/insight/content/doi/10.1108/ICS-09-2021-0145/full/html

Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski, J., & Zema, T. (2021). Cybersecurity and sustainable development. Retrieved from https://doi.org/10.1016/j.procs.2021.08.003

Zhong, C., Liu, H., & Kam, H.-J. (2023). Mining Reddit users' perspectives on cybersecurity competitions: A mixed method approach. Retrieved from https://www.emerald.com/insight/content/doi/10.1108/ICS-02-2023-0017/full/html