

# Cybersecurity Workforce Landscape, Education, and Industry Growth Prospects in Southeast Asia

Journal of Tropical Futures

1–19

© The Author(s) 2023



Article reuse guidelines:

[sagepub.com/journals-permissions](https://sagepub.com/journals-permissions)

DOI: 10.1177/27538931231176903

[journals.sagepub.com/home/jtf](https://journals.sagepub.com/home/jtf)

Roberto Dillon<sup>1</sup>  and Kim-Lim Tan<sup>2</sup> 

## Abstract

Given the chronic lack of qualified professionals in the cybersecurity industry, the present paper seeks to evaluate the current interest in cybersecurity across Southeast Asia nations and then compare it with the available educational offerings of related degrees in each country to identify eventual gaps in the market. The goal is to assess whether there is a need for additional degree programs in cybersecurity and to evaluate the potential for future growth in the industry by providing a solid educational foundation for aspiring professionals. To estimate current interest from prospective students and professionals in cybersecurity across each country, leaderboards from the popular TryHackMe gamified cybersecurity training platform are referenced. We further discuss issues by considering the related formal education programmes offered by the top universities in each country, identified by their presence in the QS world university rankings. The data are then used to propose two new metrics: the ‘Cybersecurity Education Prospects Index’ (CEPI) and the ‘Cybersecurity Industry Prospects Index’ (CIPI), which show how most of the eleven countries in Southeast Asia do have an unmet demand for cybersecurity education and only a few of

<sup>1</sup>School of Science and Technology, James Cook University Singapore, Singapore, Singapore

<sup>2</sup>JCUS Business School, James Cook University Singapore, Singapore, Singapore

## Corresponding Author:

Kim-Lim Tan, JCUS Business School, James Cook University Singapore.

Email: [Kimlim.tan@jcu.edu.au](mailto:Kimlim.tan@jcu.edu.au)

them have already developed an educational infrastructure that is ready to support the growing needs of the local and international industry.

**Keywords**

cybersecurity, technology acceptance model, cybersecurity education prospects index, cybersecurity industry prospects index, Higher Education

**Introduction***Background*

Cybersecurity is a complex and multifaceted issue faced by almost every industry. The proliferation of digital transformation requires a new approach to investing in the teams and resources needed to address this ever-changing landscape (Kuah and Dillon, 2021). We need more professionals from diverse backgrounds to fill cybersecurity roles and increase the availability of security training throughout the global workforce. Yet, it is not new information that the cybersecurity industry has experienced a chronic lack of a qualified workforce. According to the International Information System Security Certification Consortium (ISC<sup>2</sup>), it is estimated there is a shortage of 3.4 million in the cybersecurity workforce worldwide (ISC<sup>2</sup>, 2022). Within the tropical region, in particular, the Southeast Asia (SEA) region, such a lack of workforce is even more pronounced (Othman, 2022). What makes the situation more precarious is that while most companies realise the need for business transformation to stay competitive, they fail to realise that migrating to new systems, services, and offerings needs to be done securely. A survey by Trend Micro (2022) further supported this proposition, revealing that 90% of information decision-makers believed their management was willing to compromise cybersecurity in favour of digital transformation, productivity, or other goals. Additionally, the same report highlighted that 82% of IT practitioners have felt pressured to downplay the severity of cyber risks to their board (Trend Micro, 2022). Given these developments, it is not surprising when Othman (2022) highlighted that organisations in Asia are a hotbed of cyber security attacks, and 1.2 million skilled cybersecurity professionals are needed in this region.

By taking all this into account, this paper, through the popular TryHackMe (THM) gamified cybersecurity training platform, aims to define a new way to evaluate the current stance<sup>1</sup> and future prospects in the cybersecurity

landscape for each SEA country (i.e., Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, Timor-Leste, Vietnam) by answering the following three questions:

1. Does the industry have a reliable pool of graduates to source talent from?
2. Are the top local universities providing enough courses to train new talent?
3. Is there enough interest among prospective students and workers to learn about cybersecurity and enrol in the degrees being offered?

## Literature Review

### *Overview of the Cybersecurity Workforce Landscape*

The lack of expertise in this field was even more evident during and after the COVID-19 pandemic when we witnessed sudden changes in workplace practices that gave cybercriminals many new opportunities to attack unsuspecting workers online (Gillard, 2022). Moreover, it has also been reported that the few qualified people working in the industry are often prone to burnout due to the constant stress they are subjected to, as reported by Hughes (2022). This trend means that the industry is at risk because it cannot find new talents and may lose the few experienced ones it managed to hire.

Simultaneously, there has been a surge in the activities of cybercriminals. According to cyber security companies like Fortinet (2023), Kaspersky (2023), and Imperva (2023), cyber attacks occur continuously across all countries worldwide. Recent reports (see Table 1) have revealed that each country faces thousands or even millions of daily cyber threats in South East Asia, as per available data.

### *Need for Connection with Academia*

Hence, for the cybersecurity industry to thrive and deliver on its security objectives, it is of paramount importance to establish proper connections

**Table 1.** Number of Incoming Cyber Attacks on 14/2/23 Reported for Each Country by Imperva (Data Retrieved on 15/2/23).

	Malaysia	Singapore	Thailand	Indonesia	Philippines	Vietnam
Attacks	26,262,448	5,953,660	1,840,946	1,052,938	1,036,257	330,241
	<b>Myanmar</b>	<b>Cambodia</b>	<b>Laos</b>	<b>Timor-Leste</b>	<b>Brunei</b>	
	3,528	2,877	NA	NA	NA	

with academia and be sure that universities can effectively train young talent to gradually but constantly fill the ranks of white-hat hackers worldwide. To this end, the World Economic Forum (WEF) highlighted two leading skills gaps in developing the cybersecurity workforce – soft skills and cloud computing knowledge (WEF, 2022).

*Soft skills training.* According to ISACA's ('Information Systems Audit and Control Association') research, soft skills such as communication, flexibility, and leadership represent the most significant skills gap identified by cybersecurity professionals (ISACA, 2022). Therefore, building and filling open cybersecurity roles would require recruiting cybersecurity professionals from diverse backgrounds that can bring these soft skills to the fore. According to Tan and Yeap (2021), organisations should be proactive in reaching out to multiple sources in identifying diverse sets of candidates, setting up engagement strategies that can attract and retain talent from diverse backgrounds, as well as building a collaborative environment that fosters a problem-solving approach that removes traditional barriers of career advancement.

*Cloud computing knowledge.* The ISACA (2022) survey showed that cloud computing is the second largest gap among cybersecurity professionals after soft skills. Other notable gaps include security controls implementation, coding, software development, data-related, and networking-related topics.

From the above, it is evident that cybersecurity is not an easy subject to learn, as it is highly technical and requires many prerequisites to be adequately understood and applied effectively. The inherent challenges of the topic make this field particularly demanding, and only passionate and fully engaged individuals can successfully commit to a lifelong learning journey involving both formal and continuous education and sustain the constant pressure they will be subjected to once in the workforce.

In the last few years, we have observed the emergence of several cybersecurity-related portals that aim to promote the industry and engage a diverse audience, including students, hobbyists, and professionals. These portals offer a gamified platform for individuals to learn new topics or better understand foundational subjects. Moreover, they allow individuals to apply their newly acquired skills by safely and legally hacking dedicated virtual machines. THM is one of the most popular and free online platforms today, boasting a user base of more than 1.7 million registered members worldwide as of the time of writing (Gillard, 2022).

By providing themed skill paths and breaking down complex topics into bite-sized rooms that can be completed step-by-step, often in less than an hour, THM has been very successful in engaging many users for several years already, so much so that leader boards by country can now give us

valuable insights about how popular studying and practicing cybersecurity is in each country. We can then relate such information to the relevant academic offerings and propose possible metrics for evaluating the effectiveness of cybersecurity education and industry ecosystems and their prospects for the future.

### *Overview of TryHackMe (THM)*

Points, badges, and leaderboards have always been a staple in any gamified platform (Werbach and Hunter, 2012). THM is no exception. THM has 50 leaderboards updated regularly since the platform was created. These leaderboards are accessible to the public for each country. By analyzing the competition to reach the top of the leaderboard, we can gauge the level of engagement of end-users in each country. Essentially, we can estimate cybersecurity's popularity in each country. Table 2 provides the relevant data for each Southeast Asian country as of the time of writing. The standard deviation is generally high due to a few top performers and outliers. Hence, to evaluate overall engagement, the median is a more reliable metric that allows us to rank each country, as shown in Table 3.

As we can see, Vietnam appears to have the most passionate and engaged user-base in the region, followed by Indonesia and Malaysia. A median score above 30,000 points is a noteworthy indicator since an average user already needs several months of constant and hard work to reach the ultimate grade of 'God' set at 20,000 points. This result puts Vietnam above major cybersecurity powerhouses such as Israel (top 50 users median at 30,847) and Russia (median at 32,683), while still significantly behind the top leading country, which is the USA with an outstanding Top 50 median of 68,837<sup>2</sup>.

### *Factors Encouraging the Adoption of TryHackMe (THM)*

While online cybersecurity platforms such as THM are key in making cybersecurity to be accessible to a large crowd of people, more attention should be placed on encouraging its adoption. It is essential to know that making it accessible does not necessarily mean adopting the technology. In this regard, this paper argues that consumer psychology in the curriculum provides holistic subject knowledge that encapsulates different aspects of technology adoption. In the same vein, developers of such a system should be mindful of the effect on consumerism. After all, adopting a service or a product goes beyond its pure technicalities. Users' perception, comprising opinions, feelings, and beliefs, plays a large part in influencing their decision (Leong et al., 2020).

**Table 2.** Summary of Scores for Top 50 Users on THM: Basic Stats for Each SEA Country (Data Retrieved on 29/12/22. Values Rounded to the Closest Integer).

	Brunei	Cambodia	Indonesia	Laos	Malaysia	Myanmar
<b>Mean</b>	4178	11,811	30,605	2593	31,846	23,992
<b>StD</b>	6882	9418	13,348	4466	15,559	12,374
<b>Med</b>	1505	7673	27,112	548	25,426	20,569
<b>#1 user</b>	28,263	40,706	92,268	18,058	90,760	71,395
<b>#50 user</b>	416	4584	18,887	0	18,120	12,907
	<b>Philippines</b>	<b>Singapore</b>	<b>Thailand</b>	<b>Timor-Leste</b>	<b>Vietnam</b>	
<b>Mean</b>	26,324	26,462	22,485	42	40,083	
<b>StD</b>	11,113	10,390	10,707	228	18,511	
<b>Med</b>	23,547	22,223	18,998	0	33,378	
<b>#1 user</b>	79,226	60,548	77,062	1528	95,178	
<b>#50 user</b>	17,237	16,802	13,044	0	23,233	

Note: Laos and Timor-Leste have less than 50 users overall, listing only 42 and 2 users in their TOP 50 respective rankings.

**Table 3.** The 11 SEA Countries Ranked by Median Score of the Top 50 THM Performers.

#	Country	THM score
1	Vietnam	33,378
2	Indonesia	27,112
3	Malaysia	25,426
4	Philippines	23,547
5	Singapore	22,223
6	Myanmar	20,569
7	Thailand	18,898
8	Cambodia	7673
9	Brunei	1505
10	Laos	548
11	Timor-Leste	0

To this end, this section leverages the technology acceptance model (TAM) to shed further insights into different perspectives on adopting a technology. TAM is widely accepted as a model for explaining the phenomenon of adopting new technology. TAM has been anchored against perceived usefulness and perceived ease of use as the determinants of technology adoption (Davis, 1989). However, TAM has also been criticised for its parsimony and should be expanded by including factors particularly relevant to the specific technology under investigation (Schierz et al., 2010). Besides, technological advances have added layers of complexities that influence users' rate of adoption of new technologies. Specifically, studies have found that users' adoption rate is also influenced by their perceived security risk (Leong et al., 2020).

*Perceived security.* In any form of electronic services, privacy invasion has been gaining attention from users (Lwin et al., 2007). Within the cyberspace, there are many points of failure. From entering credit card details to listing delivery addresses, these are vulnerabilities where compromises could occur. Hence, in any transaction, users would need a greater sense of security when performing any online transaction.

*Perceived usefulness.* It has been recognised that perceived usefulness plays a vital role in influencing the proliferation of innovation (Tan et al., 2019). From TAM's point of view, perceived usefulness is a key construct that influences one's intention of usage, representing users' belief that innovation provides a unique advantage compared to existing change (Bazelais et al., 2017).

*Perceived ease of use.* It is described as the degree of belief that a system can be used relatively free of effort (Lew et al., 2020). Essentially, it reflects

how a system allows users to perform tasks faster and enhances performance. Therefore, if a user believes that technology is easy to operate, he or she will use it, but not the other way (Leong et al., 2020). In that regard, it is well expected that perceived ease of use will then have an impact on behaviour, namely, the higher a person's perception of the ease of using the system, the higher the level of utilisation of information technology

*Perceived compatibility* has been explained as the magnitude of an innovation that aligns with the prospective users' current values, past experiences, and needs (Diatmika et al., 2016). In other words, if the usage of a particular technology is not aligned with the values of the target segment of users, the adoption rate, according to TAM, would be lower than expected.

Other than the technical perceived features of the technology, individual users' psychological constructs also play a part in enhancing the adoption. While there are many psychological constructs, Leong et al. (2020) argue that personal innovation is a critical construct influencing new technology adoption. According to the diffusion of innovation theory, highly innovative individuals are the key to new technology as they develop a positive attitude towards it by collecting ample information. According to Nagarajan and Martina (2022), personal innovativeness is the degree to which an individual is relatively proactive in adopting technology over the other counterparts in society. In other words, this is the potential risk-taking ability of an individual to try something new and innovative.

## **Educational Offerings by QS Ranked Universities Across SEA**

Today, most, if not all, technology-based degrees offer students at least elective modules on cybersecurity. Nonetheless, to develop the talents needed by this growing industry, ad-hoc, specific curricula are needed. Therefore, to assess the industry's potential for future growth, it is necessary to examine the present state of academia and determine the number of leading institutions that have created specialised undergraduate or graduate programs; or, at the very least, incorporated a specific major into their broader technology-focused degrees. In this context, we are discussing only institutions with a legally recognised 'university' status in the country under discussion and included in the latest QS Global University Rankings (QS, 2022). A review of the current situation in each country follows.

### ***Brunei Darussalam***

Despite being the smallest country per population in the SEA region, Brunei can count on a high-quality academic offering. Both its QS-ranked institutions do



offer specialised programs (see Table 4). Overall, students in Brunei have access to one specialised major (SM) and three dedicated degrees (DD).

*Indonesia*

In contrast to Brunei, Indonesia, the biggest SEA country in terms of population, has only two institutions offering relevant degrees, despite having several universities listed in the QS rankings (see Table 5). Students studying in Indonesia who want to pursue a degree in cybersecurity can choose between a major in Computing degree and a dedicated masters program.

*Malaysia*

Of all the Southeast Asia countries, Malaysia has the most universities listed in the QS rankings (twenty-five). More than half offer cybersecurity-related programs, making this country the most active in the region regarding educational reach and options for aspiring professionals. As shown in Table 6, Malaysian students have access to six DD (five masters and one bachelor’s) plus twelve additional majors across ten bachelor’s programs and two masters programs. It is noteworthy to highlight how Malaysian universities offer degrees in Cybersecurity and branch out into even more specialised areas, such as digital forensics.

**Table 4.** Specialised Cybersecurity Academic Offering in Brunei Darussalam.

University	QS ranking	Degree
Universiti Brunei Darussalam	256	Bachelor of Digital Science, Major in Cybersecurity & Forensics
Universiti Teknologi Brunei	340	BSc (Hons) in Information Security Master of Science in Information Security Master of Science in Cyber Security

**Table 5.** Specialised Cybersecurity Academic Offering in Indonesia.

University	QS ranking	Degree
Bina Nusantara University	1001–1200	Bachelor in Computing, Major in Cyber Security
Telkom University	1001–1200	Masters Degree in Cyber Security and Digital Forensics

**Table 6.** Specialised Cybersecurity Academic Offering in Malaysia.

University	QS ranking	Degree
Universiti Malaya	70	Master in Cyber Security
Universiti Putra Malaysia	123	Master in Information security
Universiti Kebangsaan Malaysia	129	Master in Cyber Security
Universiti Teknologi Malaysia	203	Bachelor of Computer Science, Major in Computer Networks & Security
Taylor's University	284	Bachelor of Computer Science (Hons), Major in Cyber Security Master of Applied Computing, Major in Cybersecurity
Universiti Teknologi PETRONAS	361	Bachelor of IT (Hons), Major in Cyber Security
Universiti Utara Malaysia	481	Master of Science in Cybersecurity
Management and Science University	601–650	Bachelor (Hons) in Computer Forensic
Sunway University	601–650	Bachelor of Science (Hons) in IT, Major in Computer Networking and Security
Universiti Teknologi MARA – UiTM	651–700	Bachelor in Computer Science (Hons), Major in Computer Networks Master Of Science In Cybersecurity And Digital Forensics
Universiti Tenaga Nasional	701–800	Bachelor in Computer Science (Hons), Major in Cyber Security
Universiti Malaysia Pahang	801–1000	Bachelor in Computer Science (Hons), Major in Cyber Security
Multimedia University	1001–1200	Bachelor of Information Technology (Hons.), Major in Security Technology
Universiti Kuala Lumpur	1001–1200	Bachelor of Information Technology (Hons), Major in Computer System Security
Universiti Tun Hussein Onn Malaysia	1001–1200	Bachelor in Computer Science (Hons), Major in Information Security Master of Computer Science, Major in Information Security

### *Philippines*

Only two QS-ranked universities offer cybersecurity-related degrees in the Philippines (Table 7). Both are at the bachelor's level, and no graduate study opportunities exist.

**Table 7.** Specialised Cybersecurity Academic Offering in the Philippines.

University	QS Ranking	Degree
De La Salle University	801–1000	Bachelor of Science in Computer Science, Major in Network and Information Security
University of Santo Tomas	801–1000	Bachelor of Science in Information Technology, Major in Network and Security

**Table 8.** Specialised Cybersecurity Academic Offering in Singapore.

University	QS ranking	Degree
National University of Singapore	11	Bachelor of Technology in Computing, Major in Cybersecurity
Nanyang Technological University	19	Master of Science in Cyber Security
James Cook University	461	Bachelor of Cybersecurity

*Singapore*

It may come as a surprise that although Singapore has the highest-ranked universities in Southeast Asia, there are limited options for students who wish to pursue a cybersecurity degree from a QS-ranked institution. Specifically, there is only one dedicated undergraduate and graduate program and one major that is part of a more general computing degree (as indicated in Table 8).

*Thailand*

Among the ten QS-ranked universities in Thailand, only Mahidol University offers a dedicated masters degree. There is no cybersecurity-related bachelor’s program (see Table 9).

*Vietnam*

In Vietnam, only two out of the five QS-ranked Vietnamese universities are offering relevant degrees (see Table 10).

**Table 9.** Specialised Cybersecurity Academic Offering in Thailand.

University	QS ranking	Degree
Mahidol University	256	Master of Science in Cyber Security and Information Assurance

**Table 10.** Specialised Cybersecurity Academic Offering in Vietnam.

University	QS ranking	Degree
Duy Tan University	801–1000	Bachelor of IT, Major in Network Security
Hanoi University of Science and Technology	1201–1500	Bachelor in Cyber Security, Master in Computer Network and Information Security

**Table 11.** Overall Number of Dedicated Degrees (DD) and Specialised Majors (SM) per Country.

	Brunei	Indonesia	Malaysia	Philippines	Singapore	Thailand	Vietnam
DD	1	1	6	0	2	1	2
SM	3	1	12	2	1	0	1

## Others

The remaining countries such as Cambodia, Laos, Myanmar, and Timor-Leste, do not have any universities listed in the QS Rankings in 2023. A summary of the current educational landscape in terms of DD and SM, including both postgraduate and undergraduate programs, is presented in Table 11.

## Discussion

Looking at Table 11, especially when considering the results from Table 3, allows us to make some interesting observations.

First, Malaysia is the clear frontrunner when it comes to cybersecurity education, so much so that it may have no room left for further growth in the space as, despite the many degrees offered, fewer people engage in online cybersecurity activities compared to nearby countries, as shown by the THM statistics. The smallest country in the region, Brunei Darussalam,

comes a distant second in the number of degrees offered and here, too, there seems to be not much room for additional growth as young people online do not seem mainly engaged. Here, the offer seems to be already exceeding the demand.

Conversely, the level of online participation in cybersecurity in Vietnam and Indonesia is remarkable, as is the participation of users from Myanmar, a country without any QS-ranked institution but with a similar number of users in the THM pool compared to nearby countries that offer specialised programs at prominent institutions. However, to gain a deeper understanding, we must also consider another factor, enrolment percentage (see Table 12), which is the accessibility of education for children in school age, as reported by the UNESCO Institute for Statistics in 2022 (UNESCO Institute for Statistics, 2022).

With this, we can now define a new metric, the ‘Cybersecurity Education Prospects Index’ (CEPI) as:

$$CEPI = \frac{THM\ Score * EP}{K(1 + DD + SM)} \quad K = 100 \tag{1}$$

To evaluate the future growth prospects of cybersecurity education in a particular country, CEPI takes into consideration the THM median score and multiplies it by the EP,<sup>3</sup> to take into consideration the potential student pool, then divides it according to the number of degrees being offered scaled by a factor *K*, which we can set, for example, to 100 for simplicity.

The purpose of CEPI is to help in pointing out different situations and underlying contexts. For example, if many degrees are already compared to the student pool, a new degree may not be sustainable, which should result in a low score. On the contrary, a country with few degrees and a growing and passionate student population clearly has a much better potential to establish new successful programs and should receive a high CEPI score. Table 13 presents the ranking of the Southeast Asia countries according to CEPI results.

**Table 12.** Tertiary School Enrolment as a Percentage of all Eligible Children (EP).

	Brunei	Cambodia	Indonesia	Laos	Malaysia	Myanmar	Philippines	Singapore
EP	32.0	14.7	36.3	13.5	42.6	18.8	35.5	91.1
	<b>Thailand</b>	<b>Timor</b>	<b>Vietnam</b>					
EP	49.3	18.0	28.6					

**Table 13.** SEA Countries Ranked by CEPI.

Country	CEPI
Singapore	506
Thailand	468
Myanmar	387
Indonesia	328
Philippines	278
Vietnam	239
Cambodia	113
Malaysia	57
Brunei Darussalam	10
Laos	7
Timor-Leste	0

By considering the EP, we realise how Singapore, with an EP of 91%, can sustain further local growth in this space, as confirmed by a CEPI score of 506. Thailand and Myanmar are also countries with excellent growth prospects in the educational space, given that they have highly engaged youth and no or minimal academic offerings in this area provided by internationally ranked institutions. The presence of Myanmar in the third spot is particularly noteworthy, considering its low EP value. On the other hand, the CEPI score for countries such as Malaysia and Brunei confirms that these countries have already implemented a well-diversified offering relative to their student population, and further growth is unlikely. Countries such as Cambodia, Laos, and Timor-Leste must improve their overall access to education before growth in this space can finally happen. Good education is paramount to support the growth the industry so desperately needs, and we can define a similar index, the ‘Cybersecurity Industry Prospects Index’ (CIPI), to evaluate the prospects of industry growth as follows:

$$CIPI = \frac{THM \text{ Score } (1 + K_1 * DD + K_2 * SM)}{100 - EP} \quad K_1 = 2; K_2 = 1 \quad (2)$$

To evaluate potential industry growth, CIPI multiplies the THM median score for a factor that considers the number of degrees being offered, assigning a different weight to DD (whether undergraduate or graduate) compared to majors in more general degrees ( $K_1 = 2$  and  $K_2 = 1$ , respectively). Then it divides the result by taking into account the percentage of children who do not have access to tertiary education, i.e., countries that have a low enrolment percentage will find it more difficult to sustain industry growth since the local

**Table 14.** SEA Countries Ranked by CIPI.

Country	CIPI
Singapore	14,965
Malaysia	11,068
Vietnam	2806
Indonesia	1702
Thailand	1124
Philippines	1096
Myanmar	253
Brunei Darussalam	177
Cambodia	90
Laos	6
Timor-Leste	0

educational system will generate less fresh talent. Hence the score has to be divided by a higher number. Table 14 presents the ranking of the Southeast Asia countries according to CIPI results.

Once again, Singapore tops the ranking thanks to its very high EP value and good THM Score. Together with highly ranked institutions’ dedicated and specialised programs, it should guarantee a constant source of talent for healthy industry growth. Malaysia also scores very highly thanks to its many degrees spread around the country that should quickly push the local industry forward. A group of four countries follows, including Vietnam, Indonesia, Thailand, and the Philippines. These have all excellent potential in terms of young, engaged people who may be suitable candidates to foster industry growth. Still, the current low EP numbers and the scarcity of suitable degrees make it more challenging for the local industry to develop and fulfil its potential. Cambodia, Laos, and Timor-Leste close the ranking, and more fundamental issues must be resolved before the local cybersecurity industry can finally take off.

## Conclusions

Online cybersecurity training platforms, such as THM, are essential not only to make cybersecurity accessible to a large number of people but also to gauge how interested and engaged young internet users are with technology and the opportunities it offers, hence providing us with a valuable tool to assess current and prospects for the cybersecurity world.

By factoring in various variables, such as the level of engagement of users on the platform and the availability of quality education and relevant

academic programs, we have introduced two distinct indexes, namely CEPI and CIPI. These indexes can help determine which countries are in the most advantageous position to leverage the increasing interest in cybersecurity and channel that growth into the education system initially and subsequently, into the industry.

Singapore tops the rankings in both indices, showing strong prospects in both areas, while Malaysia scores very well in CIPI but poorly in CEPI. This is an interesting result due to the abundance of degrees currently offered, which make it easy to support the local industry but will not make it a good market for further educational expansion.

On the contrary, other countries such as Vietnam, Indonesia, Thailand, the Philippines, and Myanmar are well positioned for rapid educational growth that can, later, support the industry as needed. In these scenarios, Myanmar is particularly noteworthy since there are no QS ranked Universities and hence no DD considered by the metrics, besides a very low tertiary education enrolment percentage. Yet, it can show a very receptive community of cybersecurity enthusiasts, as shown by the TOP 50 THM median score above the 'God' level threshold of 20,000 points, making this a place just waiting to emerge.

Taken together with TAM, we argue that the fundamental tenets within the model offer new insights to introduce cybersecurity trainings through online or remote mode, especially for countries that received poor CIPI and CEPI. At the same time, we do not suggest that countries that have performed well, such as Singapore and Malaysia, should ignore TAM. After all, understanding technology acceptance will lead to better prediction of the use of new information resources, even if such systems are optional or an additional conduit in providing cybersecurity training.

In other words, university administrators should not underestimate the psychological factors influencing technology adoption. In this regard, students' readability to the online learning contents, establishing the needed facilities such as a 24/7 helpline, and ensuring the portal is compatible with the different browsers are essential to minimise students' irritation in accessing online learning content as well as maneuvering across the different modules. For countries that perform relatively poorly across both CEPI and CIPI, we further advocate that events or roadshows should be organised to facilitate the students in fostering a positive attitude towards online learning. Furthermore, training courses and roadshows can be organised to foster a positive view of students' perception of the ease and usefulness of online learning could also enhance their positive attitudes and, consequently their behavioural intention.

Despite the interesting insights obtained by the analysis, we should acknowledge that this study also has limitations. Only one online platform was



discussed at a time when there are a few different contenders in the online cybersecurity gamified training space, and the educational space took into consideration only ranked institutions. We will likely miss other institutions that can significantly shape the local educational scene in each country. At the same time, future authors can also consider doing an empirical analysis of drawing relationships between different countries' cybersecurity professionals' skills, abilities and aptitude, technological acceptance, and other variables that can also be included in the analysis, such as, universities' cybersecurity educational offerings and graduates.


### Declaration of Conflicting Interests


The authors declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

### Funding

The authors received no financial support for the research, authorship and/or publication of this article.

### ORCID iDs

Roberto Dillon  <https://orcid.org/0000-0003-0166-0273>

Kim-Lim Tan  <https://orcid.org/0000-0001-8343-5103>

### Notes

1. The accuracy of the data used for analysis is valid up until 13 April 2023.
2. Data calculated on 31 December 2022
3. Divide the number of students enrolled in a particular educational institution in a given level of education by total enrolment (public and private) at the same level of education, and multiply the result by 100.

### References

- Bazelais P, Doleck T and Lemay DJ (2017) Investigating the predictive power of TAM: A case study of CEGEP students' intentions to use online learning technologies. *Education and Information Technologies* 23(1): 93–111.
- Davis FD (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly* 13(3): 319–340.
- Diatmika IWB, Irianto G and Baridwan Z (2016) Determinants of behavior intention of accounting information systems based information technology acceptance. *Imperial Journal of Interdisciplinary Research* 2(8): 125–138.

- Fortinet (2023) Threat Cloud. Available at <https://threatmap.checkpoint.com> (accessed 15 February 2023).
- Gillard E (2022) TryHackMe in Review 2022. TryHackMe Newsroom. Available at <https://tryhackme.com/resources/blog/2022-review> (accessed 29 December 2022).
- Hughes O (2022) Bad news: The cybersecurity skills crisis is about to get even worse. *ZDNet*. Available at <https://www.zdnet.com/article/bad-news-the-cybersecurity-skills-crisis-is-about-to-get-even-worse/> (accessed 29 December 2022).
- Imperva (2023) Cyber Threat Attack Map. Available at <https://www.imperva.com/cyber-threat-attack-map/> (accessed 15 February 2023).
- ISACA (2022) State of Cybersecurity 2022: Global Update on Workforce Efforts, Resources and Cyberoperations. Available at [www.isaca.org](http://www.isaca.org) (accessed 15 January 2023).
- ISC<sup>2</sup> (2022) Cybersecurity Workforce Study 2022. Available at <https://www.isc2.org/Research/Workforce-Study> (accessed 29 December 2022).
- Kaspersky (2023) Cyber Threat Real Time Map. Available at <https://cybermap.kaspersky.com/> (accessed 15 February 2023).
- Kuah A and Dillon R (2021) *Digital Transformation in a Post-COVID World: Sustainable Innovation, Disruption and Change*. Florida, US: CRC Press, 129–154.
- Leong C-M, Tan K-L, Puah C-H, et al. (2020) Predicting mobile network operators users m-payment intention. *European Business Review* 33(1): 104–126.
- Lew S, Tan GW, Loh XM, et al. (2020) The disruptive mobile wallet in the hospitality industry: An extended mobile technology acceptance model. *Technology in Society* 63: 101430.
- Lwin M, Williams J and Wirtz J (2007) Consumer online privacy concerns and responses: A power responsibility equilibrium perspective. *Journal of the Academy of Marketing Science* 35(4): 572–585.
- Nagarajan S and Martina M (2022) Exploring the marketing related stimuli and personal innovativeness on the purchase intention of electric vehicles through technology acceptance model. *Cleaner Logistics and Supply Chain* 3: 100029.
- Othman NZ (2022) Cybersecurity skills gap contributes to security breaches in Asia. *New Straits Times*. Available at <https://www.nst.com.my/lifestyle/bots/2022/07/811304/tech-cybersecurity-skills-gap-contributes-security-breaches-asia> (accessed 29 December 2022).
- QS (2022) QS World University Rankings. QS Quacquarelli Symonds. Available at <https://www.topuniversities.com/university-rankings/world-university-rankings/2023> (accessed 29 December 2022).
- Schierz PG, Schilke O and Wirtz BW (2010) Understanding consumer acceptance of mobile payment services: An empirical analysis. *Electronic Commerce Research and Applications* 9(3): 209–216.
- Tan K-L, Memon MA, Sim P-L, et al. (2019) Intention to use mobile payment system by ethnicity: A partial least squares multi-group approach. *Asian Journal of Business Research* 9(1): 36–59.

- Tan K-L and Yeap PF (2021) The impact of work engagement and meaningful work to alleviate job burnout among social workers in New Zealand. *Management Decision* 60(11): 3042–3065.
- Trend Micro (2022) 90% of IT Decision Makers Believe Organizations Compromise on Cybersecurity in Favor of Other Goals. Available at [www.trendmicro.com](http://www.trendmicro.com). (accessed 15 January 2023).
- UNESCO Institute for Statistics (2022) School enrollment, tertiary (% gross). Available at <https://data.worldbank.org/indicator/SE.TER.ENRR> (accessed 29 December 2022).
- WEF (2022) How to develop the global cybersecurity workforce and build a security-first mindset. Available at <https://www.weforum.org/agenda/2022/12/how-to-develop-the-global-cybersecurity-workforce-and-build-a-security-first-mindset/> (accessed 15 January 2023).
- Werbach K and Hunter D (2012) *For the Win: How Game Thinking Can Revolutionise Your Business*. Philadelphia, US: Wharton School Press.

### Author Biographies

**Roberto Dillon** is an IEEE Senior Member and the author of several books published by AKPeters, CRC Press and Springer. He is an Associate Professor at James Cook University Singapore where his research focuses on different topics related to cybersecurity and serious games.

**Kim-Lim Tan** is a member with the Society of Industrial and Organisational Psychology and the author of several publications with SSCI journals. He is a lecturer at James Cook University Singapore where his research focuses on different topics related to organisational psychology.