ASEAN's Resilience in Capacity Building

With the evolving cyberthreats that pose danger to the economic and social aspects of life in this time of digital transformation, especially when a sufficient cybersecurity workforce is still in the making, in 2018, the Government of Japan and the Association of Southeast Asian Nations (ASEAN), which is a union of 10 Southeast Asian member states including Brunei, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam, agreed to establish the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC)[1] to train at least 700 cybersecurity personnel to counter cyberthreats and close the cybersecurity skills gap.

Prior to 2020, AJCCBC, like many other training centers, enhanced the capacity of their cyberpersonnel by conducting in-person training. However, after the emergence of COVID-19, AJCCBC was unable to continue their in-person trainings and had to adapt. By migrating training to online platforms, which was new to both the trainers and trainees, AJCCBC was able to become resilient and continue capacity building to close the cybersecurity skills gap. Despite the COVID-19 outbreak, the AJCCBC was able to strengthen its cybersecurity capacity in the region by conducting 17 training sessions, four Cyber SEA Games events and two workshops for 734 ASEAN Member State (AMS) participants by the end of 2021. To transform what is already effective to something new in times of change, dedication and flexibility from operation and management teams are imperative.

Project Background

The AJCCBC project was approved at the 17th ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN) in November 2017 in Siem Reap, Cambodia.[2] The project is funded by the Government of Japan and ASEAN through the Japan-ASEAN Integration Fund (JAIF 2.0) to enhance the cybersecurity capacity of at least 700 ASEAN personnel from government sectors and critical information infrastructures (CIIs).

The First Stage

From mid-2018 until early 2020, AJCCBC conducted instructor-led training sessions focused on

THONGCHAI SANGSIRI | SECURITY+

Is an expert on cybersecurity and international cooperation at the Electronic Transactions Development Agency under the Ministry of Digital Economy and Society (Thailand). He has spent 10 years in the public sector managing and supporting various governmental information and communication technology initiatives and security awareness training programs.

ARAYA SAWASDICHAI | CISM, CDPSE, CISSP

Has been working in the government sector for 10 years. His areas of proficiency include national policies, technical knowledge, law and regulation enforcement. He is currently responsible for managing cybersecurity programs and coordinating capacity-building projects with domestic stakeholders and international partners.

ISSARA AMORNKRAISEE

Started his career with ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) as an administrative associate and is now an assistant program manager. He has been operating and coordinating this project for more than a year.

KAMONCHANOK CHAIYAKUN

Is an administrative associate on this project.

© 2022 ISACA. All rights reserved. *www.isaca.org*

incident response (e.g., CYber Defense Exercise with Recurrence [CYDER]),[3] network forensics and malware analysis at its training facility in Bangkok, Thailand. The regular format of in-person training ensured that participants could engage by physically interacting with each other and working collaboratively in groups to create strong connections among personnel. Moreover, onsite training provides direct and instant interaction between instructors and participants; it is easy to ask and answer questions, discuss the course material and problem solve. Also, recognizing the important role the younger generation plays in the cybersecurity field to strengthen cybersecurity in the region, AJCCBC conducts Cyber SEA Games annually to challenge participants. The winning teams from 2018–2021 were Indonesia, Thailand, Singapore and Thailand again, respectively (**figure 1**).

Time for Resilience

When COVID-19 restrictions were imposed, AJCCBC had to stop conducting in-person training. In late 2020, AJCCBC decided to utilize online platforms

FIGURE 1

AJCCBC Overview

Source: ASEAN-Japan Cybersecurity Capacity Building Centre. Reprinted with permission.

© 2022 ISACA. All rights reserved. www.isaca.org

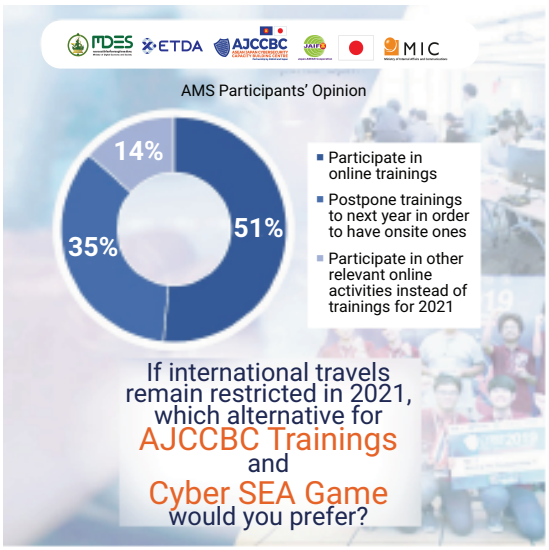
such as virtual meeting rooms, which required changes to the format of the training sessions. To make the online-first exercises more suitable to the new normal, interactive dashboards to support users' actions and increase participant engagement were added.

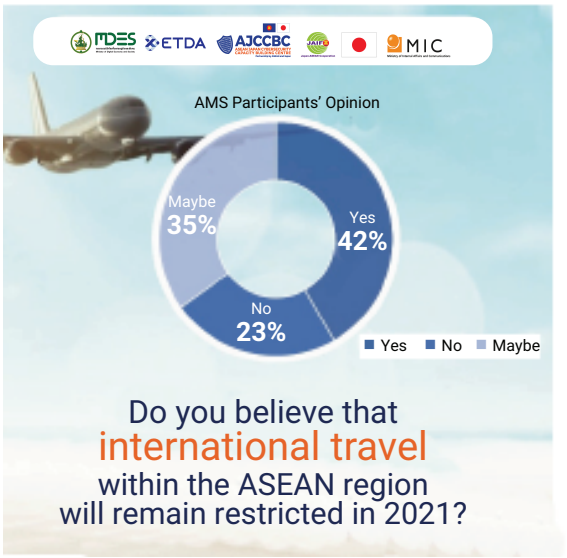
After in-person training was halted, AJCCBC conducted a survey to assess cybersecurity training needs and opinions regarding the pandemic.[4] The survey had 103 AJCCBC alumni respondents and, as shown in **figure 2**, the results suggested that:

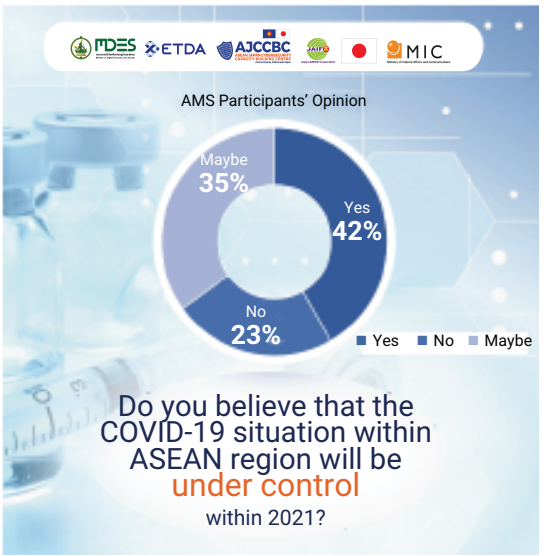
- Seventy-seven percent of respondents answered yes or maybe to whether they believed that international travel within the ASEAN region would remain restricted in 2021.
- Seventy-seven percent of respondents answered yes or maybe to whether they believed that the COVID-19 situation would be under control by 2021.
- Fifty-one percent of respondents supported the idea of having training and Cyber SEA Games conducted online.
- Forty-two percent of respondents considered online activities to be sufficiently effective.

FIGURE 2

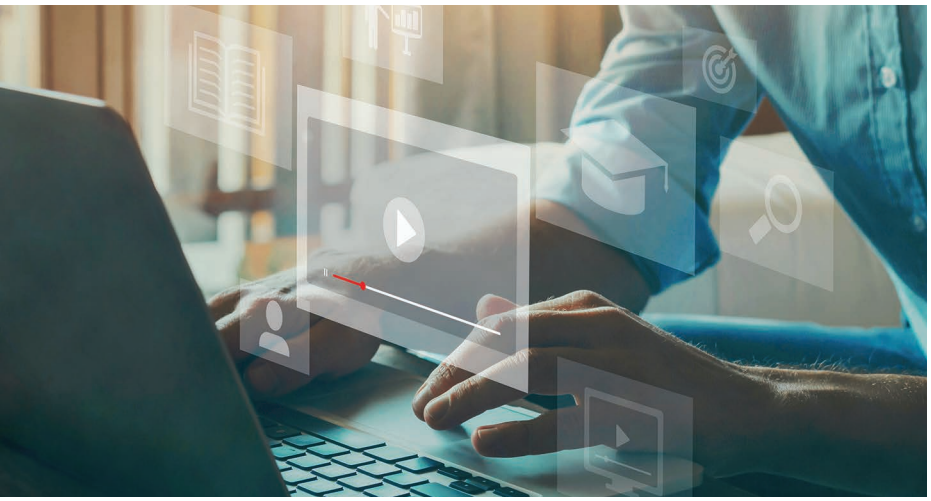
AJCCBC Survey on COVID-19 and Cybersecurity Training







© 2022 ISACA. All rights reserved. *www.isaca.org*



AJCCBC has continued its activities virtually since November 2020, with seven online training courses, two Cyber SEA Game events and one workshop for 378 participants.

Despite the effects of the pandemic, AJCCBC's objectives remain unyielding in alleviating the cybersecurity workforce shortage in the ASEAN region. AJCCBC has four value propositions:

1. Act as a regional participant broker in disseminating knowledge to the participants.
2. Close the cybersecurity skills gap by tailoring cybersecurity courses to cover many topics, such as incident response, malware analysis, digital forensics, cybersecurity awareness and executive cyber leadership. These courses are available for technical and management roles.
3. Act as a cybersecurity workforce source by researching and reporting ASEAN cybersecurity workforce shortage information, skill demands and insight on the ASEAN cybersecurity profile.
4. Create and maintain relationships with trained personnel by offering online platforms to help them engage with each other and advance their careers.

Given the value of such activities, AJCCBC could be a prototype or a role model for other areas; however, norms and cultures of those areas should be considered when implementing a similar program. Most important, resilience in achieving the desired values of an entire region should not be disregarded. The countries in a particular region are connected in terms of culture, economy and society—all of which rely not only on physical infrastructure, but digital infrastructure as well. Therefore, having resilience in capacity building is a crucial strategy to maintain a region's functionality and sustain its prosperity.

Moving Forward

After learning that the online training format did not profoundly affect the quality of learning for the participants, AJCCBC continued to explore new learning formats such as microlearning and self-learning courses, where the participants can learn from anywhere and anytime at their convenience. Before implementing these new formats, AJCCBC needed to identify what content was best to apply to each format.

To measure the change in demands and understand what would be most beneficial to ASEAN, AJCCBC conducted the AJCCBC Cybersecurity Workforce Survey 2021, which was completed by 76 AJCCBC alumni from ASEAN Member States (AMS) (**figure 3**).[5]

> Having resilience in capacity building is a crucial strategy to maintain a region's functionality and sustain its prosperity.

The majority of cybersecurity personnel who completed the survey worked in info/telecommunication at a cybersecurity agency or on a computer emergency response team (CERT). In addition, 81 percent had been working in the cybersecurity field for less than 10 years. In terms of gender, 82 percent of survey respondents are male, while the remaining 18 percent are female, which might suggest a potential gender disparity in cybersecurity within the region. The results of the survey suggest that the cybersecurity areas that require improvement are incident investigation and response, cloud computing security, and security awareness. The survey also indicates that the three most in-demand skills in cybersecurity are threat intelligence analysis, penetration testing and security analysis.

Based on these results, AJCCBC took the opportunity to expand its content to include establishing CERTS and cybersecurity awareness to help

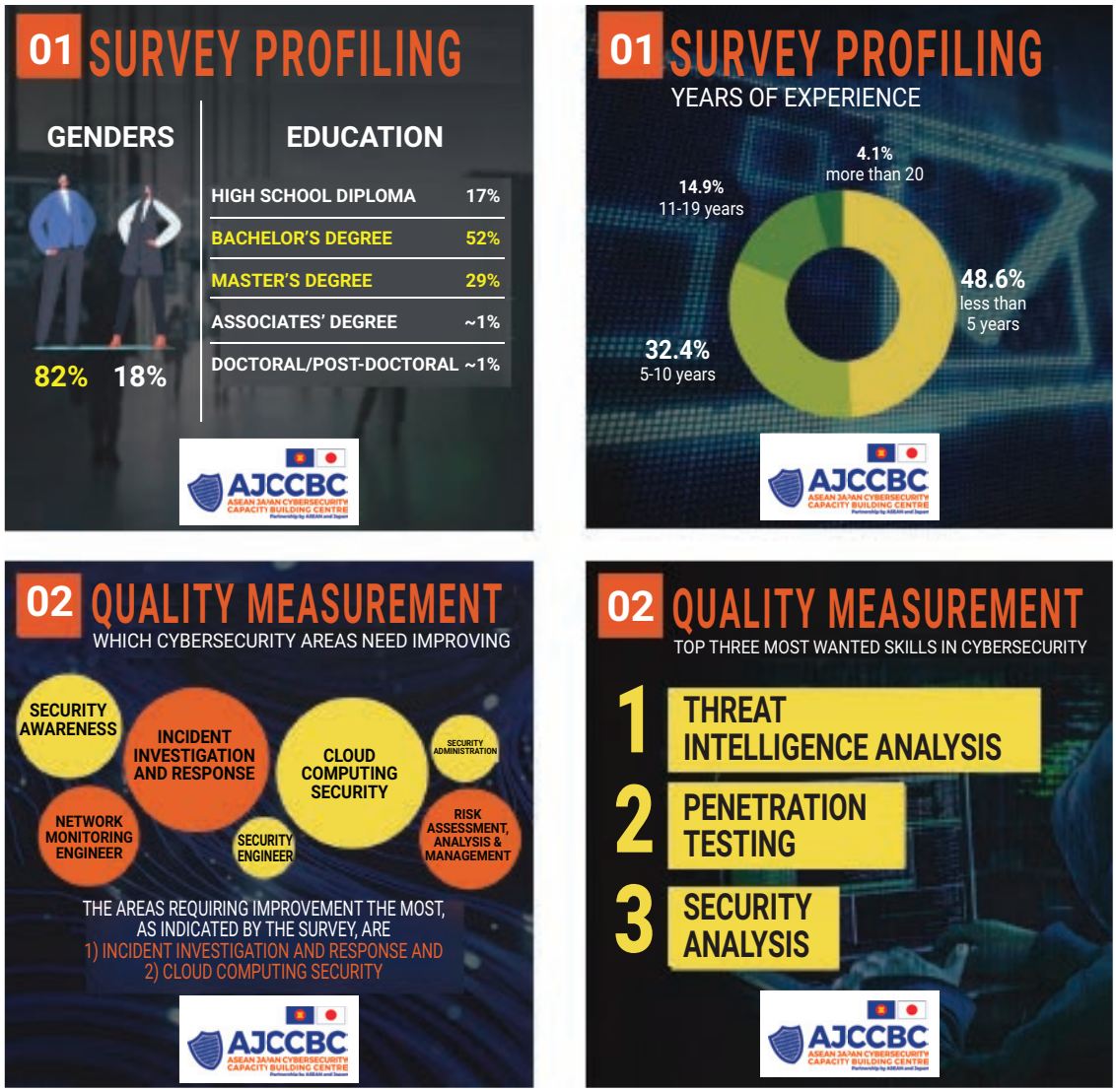
LOOKING FOR MORE?

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

© 2022 ISACA. All rights reserved. *www.isaca.org*

FIGURE 3

ASEAN-Japan Cybersecurity Workforce Survey



strengthen resilience in capacity building, especially during a pandemic.

AJCCBC also created a virtual tour to recall the experiences of past trainees during their time in physical training sessions and introduce new participants to the AJCCBC alumni circle during the pandemic.[6]

Training Evaluation

The technical knowledge and skills of the trained personnel should be measurable to evaluate the effectiveness of the trainings. To do so, AJCCBC evaluated AMS participant improvement by conducting two tests (a pretest and a post-test) of three main courses, consisting of incident response (CYDER), network forensics and malware analysis. The pretest was conducted prior to the training sessions and the post-test was conducted on the last day of the training. As shown in **figure 4**, it can be concluded that personnel's capacity was greatly enhanced by the training.[7] This is important to monitor because there is a potential risk of lack of interest in the courses in the future because the training, whether in person or online, has been provided for nearly five years. Measuring the effectiveness of these training sessions is important to help guide the future direction of the program.

© 2022 ISACA. All rights reserved. *www.isaca.org*

FIGURE 4

AMS Cyberimprovement

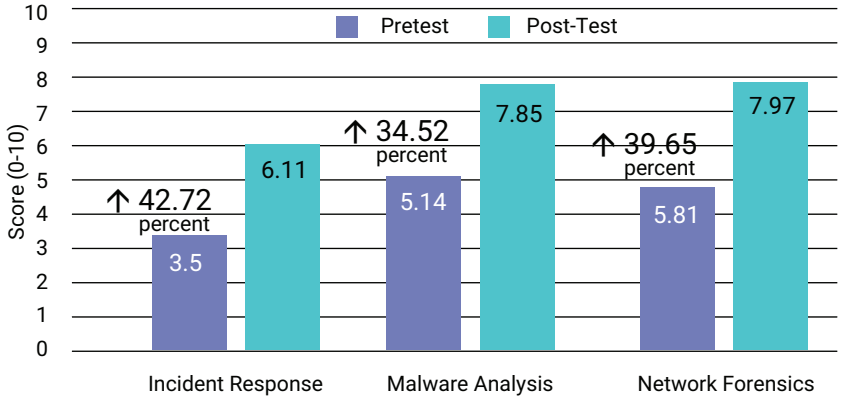
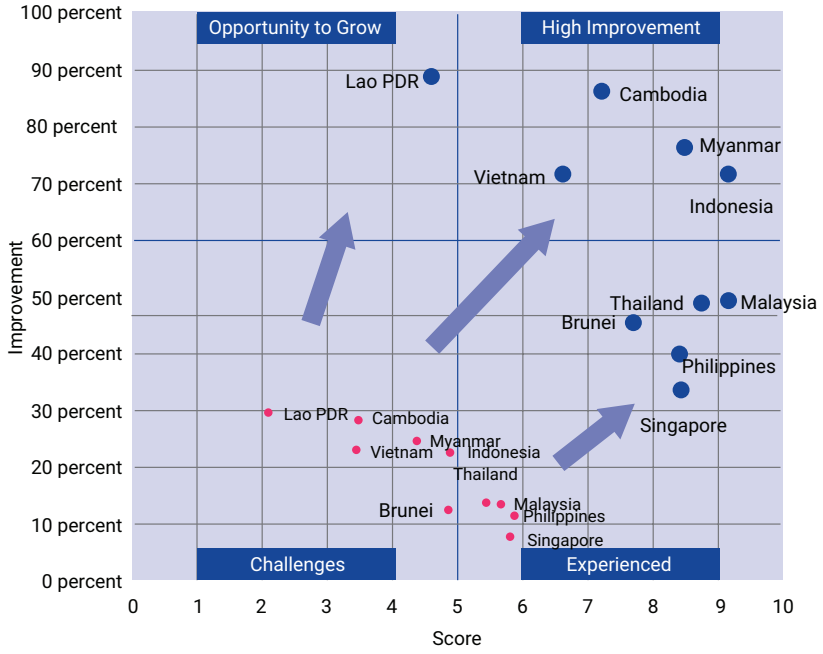


FIGURE 5

AMS Cyberimprovement by Country



To assess the improvement of AMS participants by country, AJCCBC collected samples of the training results from four training sessions (onsite and virtual) with a total of 131 participants across ASEAN (**figure 5**). The red plot shows the pretest average score for each country, while the blue plot shows the post-test average score.

The scatter graph allows each country to be placed into one of the four improvement quadrants: opportunity to grow, high improvement, experienced and challenges.

1. **Opportunity to grow**—Lao PDR is the only country in this group. Its post-test score is least improved compared to the pretest. However, it is still possible that the participants from Lao PDR might be improved after the next trainings.
2. **High improvement**—Cambodia, Indonesia, Myanmar and Vietnam, whose improvement in the post-test is remarkable, are included in this group.
3. **Experienced**—Participants from Brunei, Malaysia, Philippines, Singapore and Thailand had high scores in both the pretest and post-test; it can be assumed that the personnel of these counties have great capacity in cybersecurity.
4. **Challenges**—The challenges group has the lowest pretest scores. With proper knowledge transfer, they can grow to be included in the other groups.

Microlearning Results

Despite being affected by COVID-19, AJCCBC successfully conducted cybersecurity online training within ASEAN. To strengthen cybersecurity workforces in AMSs, AJCCBC provided a free online self-learning course titled Establishing a CSIRT, which concentrates on how to establish an effective computer security incident response team (CSIRT) via the EdApp platform.[8]

The course took place from 1 November–31 December 2021 with 101 participants; however, only seven out of 101 learners completed the course material. Therefore, AJCCBC plans to utilize new strategies, such as sending a reminder via EdApp direct message on the first day of the course, then the seventh, 21st and 60th day, to achieve a course completion rate of 90 percent and conduct review sessions with participants to increase the learner engagement in the next microlearning courses.

AJCCBC proposed these two mitigation plans in the Project Steering Committee (PSC) meeting and obtained approval to proceed. Moreover, providing a Certificate of Completion is another key step that the PSC recommended to encourage the participants.

© 2022 ISACA. All rights reserved. www.isaca.org

Next Steps

Acknowledging the importance of capacity building and their past achievements in having trained more than 700 personnel, AJCCBC proposed a new project titled Project for Enhancing ASEAN-Japan Capacity Building Programme for Cybersecurity and Trusted Digital Services to carry on its mission in providing training and other cyber-related activities to fulfill ASEAN cybersecurity capacity-building ongoing demands.

AJCCBC intends to provide capacity-building programs in three ways to address AMS training demands:

1. Collaborate with international experts and acquire knowledge
2. Share that knowledge with AMSs through onsite and online activities including training courses, Cyber SEA Games, workshops, conferences and seminars
3. Share lessons learned, best practices and accomplishments with the international cybersecurity community

Currently, the project has been successfully implemented with support and collaboration from ASEAN Member States, the ASEAN Secretariat,[9] the Ministry of Internal Affairs and Communications of Japan,[10] the Mission of Japan to ASEAN,[11] the JAIF Management Team,[12] the Embassy of Japan in Thailand,[13] the Ministry of Digital Economy and Society,[14] and the Electronic Transactions Development Agency.[15]

Conclusion

To establish resilient capacity building in the ASEAN region due to the impact of the COVID-19 pandemic, AJCCBC conducted subjective measurements through surveys and qualitative measurement through the assessment of the participant improvement in the cybersecurity field. During the early stages of the online format, AJCCBC went through a process of trial and error to find the most effective way to provide AJCCBC online activities to AMS participants.

AJCCBC has applied a plan-do-check-act (PDCA) security program to address travel restrictions during COVID-19 in the ASEAN region. Other areas of the world may adopt the region's resilience in capacity building. Regardless of where these types of programs are implemented, it is essential that the program include effective measurement and evaluation, allowing feedback from participants to the management team. Then, the management team can capture the most efficient action items and act on them or seek assistance from partners accordingly.

During the early stages of the online format, AJCCBC went through a process of trial and error to find the most effective way to provide AJCCBC online activities to AMS participants.

Endnotes

1 Association of Southeast Asian Nations (ASEAN)-Japan Cybersecurity Capacity Building Centre, *https://www.ajccbc.org/*

2 Association of Southeast Asian Nations (ASEAN), "The 17th ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings," 1 December 2017, *https://asean.org/wp-content/uploads/2012/05/14-TELMIN-17-JMS_adopted.pdf*

3 Ministry of Internal Affairs and Communications of Japan, "Implementation CYber Defense Exercise with Recurrence (CYDER) for Local Governments," 19 July 2016, *https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2016/7/19_01.html*

4 Association of Southeast Asian Nations (ASEAN)-Japan Cybersecurity Capacity Building Centre, "AJCCBC Survey on COVID-19 Situation and Cybersecurity Training," 12 July 2021, *https://www.facebook.com/AJCCBC/posts/321363983006607*

5 Association of Southeast Asian Nations (ASEAN)-Japan Cybersecurity Capacity Building Centre, "AJCCBC Cybersecurity Workforce Survey 2021," 23 August 2021, *https://www.facebook.com/AJCCBC/posts/347545343721804*

6 Association of Southeast Asian Nations (ASEAN)-Japan Cybersecurity Capacity Building Centre, Virtual Tour, *https://go.ajccbc.org/virtual-tour*

© 2022 ISACA. All rights reserved. *www.isaca.org*

7 Japan-ASEAN Integration Fund (JAIF), "Enhancing Cybersecurity Skills of Professionals in ASEAN," 3 November 2021, *https://jaif.asean.org/beneficiaries-voice/enhancing-cybersecurity-skills-of-professionals-in-asean/*
8 The Mobile Learning Management System, EdApp: The Mobile LMS, *https://www.edapp.com/*
9 Association of Southeast Asian Nations (ASEAN), "The ASEAN Secretariat: Basic Mandate, Functions and Composition," *https://asean.org/the-asean-secretariat-basic-mandate-functions-and-composition/*
10 Ministry of Internal Affairs and Communications, Japan, *https://www.soumu.go.jp/english/*
11 Mission of Japan to ASEAN, *https://www.asean.emb-japan.go.jp/itprtop_en/index.html*
12 Japan-ASEAN Integration Fund (JAIF), "JAIF Management Team," *https://jaif.asean.org/jmt/*
13 Embassy of Japan, Thailand, *https://www.th.emb-japan.go.jp/itprtop_en/index.html*
14 Ministry of Digital Economy and Society, *https://www.mdes.go.th/*
15 Electronic Transactions Development Agency, *https://www.etda.or.th/*

© 2022 ISACA. All rights reserved. *www.isaca.org*