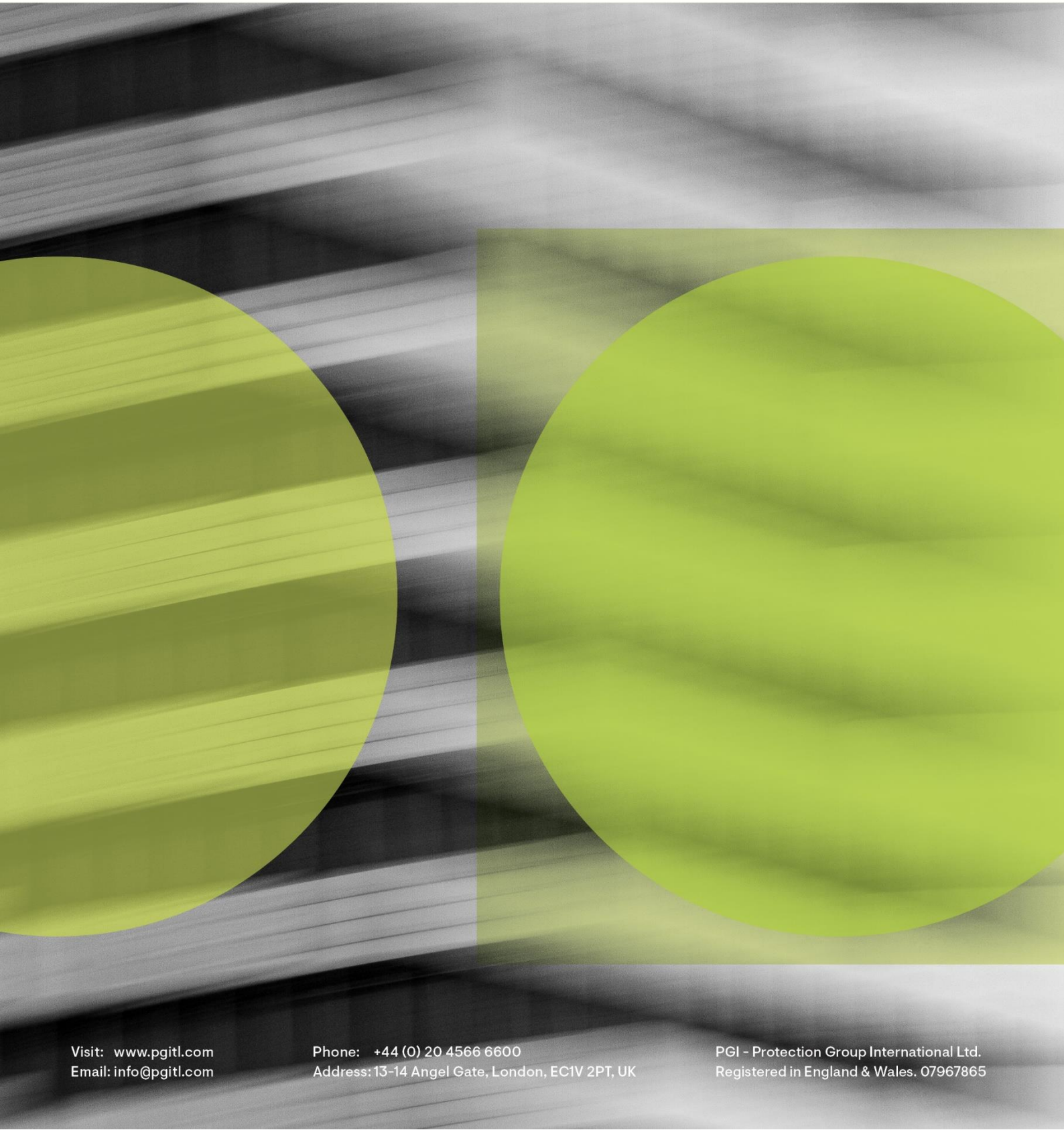
Final Report

Women's Participation in Southeast Asia's Cybersecurity Sector

August 2024



Visit: www.pgitl.com
Email: info@pgitl.com

Phone: +44 (0) 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT, UK

PGI - Protection Group International Ltd.
Registered in England & Wales. 07967865

Table of Contents

August 2024 1

Acknowledgements 1

Executive Summary 2

Introduction 4

Background 4

Approach 4

Chapter 1: Strategic Drivers 6

Introduction 6

Methodology 6
Data Collection 6
Research Participants 6
Research Limitations 7

Analysis of Strategic Drivers 8
Principal National Cybersecurity Risks 8
Digital Transformation 10
Legislation and Regulation 13
Critical National Infrastructure 17
National Security and Criminal Justice System 19
Incident Response 23
Security Standards and Controls 26
National and Regional Cooperation 29
Research and Development 31

Conclusion 33

Chapter 2: Participation of Women in the Cybersecurity Workforce 34

Introduction 34

Methodology 34
Data Collection 34
Research Participants 34
Research Limitations 34

General cybersecurity workforce situation 35
National Workforce Context 35
Challenges for Workforce Development 36
Current Initiatives 36
Insights from Existing Research 37

Participation of Women in the Cybersecurity Workforce 38
Current participation levels 38
Perceived benefits 38
Barriers and challenges 39
Participation and retention activities 40

Ideas and recommendations for future interventions 41
Insights from Existing Research 42

Conclusion **43**

Chapter 3: Future Workforce Assessment 44

Introduction **44**

Methodology **44**
Assessment Approach 44
National cybersecurity capacity maturity 45
Cybersecurity Workforce and Skills Frameworks 46

Southeast Asia Cybersecurity Future Workforce Assessment **48**
Cybersecurity Workforce Functions and Teams 48
Priority Technical Cybersecurity Roles 50
Additional Cybersecurity Workforce Requirements 53
Participation of Women in the Future Cybersecurity Workforce 53

Conclusion **54**

Chapter 4: Market Assessment 55

Introduction **55**

Summary of Market Assessment Findings **55**

Methodology **56**
Overview 56
Sources 56
Key Words 56

Market Assessment Findings **57**
Regional Efforts 57
Cambodia 58
Indonesia 66
Laos 74
Mongolia 80
Thailand 85

Conclusion **92**

Chapter 5: Gap Assessment 93

Introduction **93**

Methodology **93**

Gap Assessment Findings **94**
Cambodia 94
Indonesia 96
Laos 98
Mongolia 99
Thailand 100
Regional View 104

Conclusion **105**

Key Findings and Recommendations 106

Summary of Key Findings **106**
Opportunities 106
Challenges 109

Recommendations **111**
Recommendations for Capacity Building Intervention Design Strategies 111
Recommendations for Capacity Building Intervention Principles and Approaches 115

Acknowledgements

The Women's Participation in Southeast Asia's Cybersecurity Sector project is part of the USAID's Digital Asia Accelerator project which aims to increase the safe and appropriate use of digital technology for economic development in Southeast Asia and Mongolia.

This project was managed by Development Alternatives Incorporated (DAI) and completed by Protection Group International (PGI).

This research project was conducted as part of the USAID and International Telecommunication Union (ITU) joint declaration on promoting gender equity and inclusion in cybersecurity for Asia and the Pacific. [1]

The project team would like to thank the national and regional stakeholders who participated in this research for their valuable contributions, including focal points from the Ministry of Post and Telecommunications Cambodia (MPTC), National Cyber and Crypto Agency (BSSN) Indonesia, Lao Computer Emergency Response Team (Lacer), Ministry of Digital Development and Communications (MDDC) Mongolia, and the National Cyber Security Agency (NCSA) Thailand.

[1] https://www.usaid.gov/asia-regional/press-releases/dec-15-2022-usaid-and-itu-join-hands-promote-gender-equity-and-inclusion-cybersecurity-asia-and-pacific

Executive Summary

Women's Participation in Southeast Asia's Cybersecurity Sector

BACKGROUND

This report compiles the research findings from the Women's Participation in Southeast Asia's Cybersecurity Sector project which was completed to understand the cybersecurity workforce in Cambodia, Indonesia, Laos, Mongolia and Thailand, identify gaps in the workforce to equip these five countries with the cybersecurity requirements of the future, and understand women's participation in the sector across these five geographies. The research has also been completed in support of the ITU's Women in Cyber (WiC) Mentorship Asia-Pacific Programme and lays the foundation for future iterations of the Programme through data driven targeted capacity and skills development.

REPORT CHAPTERS

Chapter 1: Strategic Drivers describes activities and capabilities across the five focus countries which are either already planned or which are likely to be required in the next five years to mitigate risks or build maturity alongside the main existing, planned or anticipated regulatory drivers.

Chapter 2: Participation of Women in the Cybersecurity Workforce presents insights on the current cybersecurity workforce context and the participation of women in the cybersecurity workforce in the Southeast Asian region.

Chapter 3: Future Workforce Assessment presents a high-level assessment of the future workforce requirements of the five research focus countries based on the nine strategic drivers identified in the Strategic Drivers chapter and extrapolates priority technical cybersecurity roles.

Chapter 4: Market Assessment presents a market assessment of the current cybersecurity skills base in each of the five research focus countries organised into four categories of (i) Primary and Secondary School, (ii) Higher Education and Research, (iii) Professional Training and Certification, and (iv) Public and Executive Awareness.

Chapter 5: Gap Assessment combines the findings from the future workforce assessment (demand-side of cybersecurity workforce ecosystem) and the market assessment (supply-side) to produce an assessment to understand the gap between the anticipated skill requirements and current training capability and capacity.

KEY FINDINGS

OPPORTUNITIES

Full-Utilisation of the Labour Market
Rapidly increasing the participation of women into can help countries respond to strategic drivers and support the full-utilisation of the labour market.

Wide-Ranging Benefits across Society
National benefits from increasing the participation rate of women in the cybersecurity workforce can include societal level benefits such as more effective cybersecurity solutions, positive impact of a diverse workforce, improved threat mitigation, inspiring future generations. breaking stigmas and increasing resource base. In addition, benefits to be gain by women themselves can include higher salaries and familial stability.

Defined Future Workforce Roles and Training Pathways
Through clearly identifying and defining priority technical cybersecurity roles, there is an opportunity for countries to develop informed workforce development policies and activities.

Building on existing Education and Training Market
With cybersecurity already established as part of the education and training market across the five research focus countries, there is an opportunity to build on this foundation and explore efforts to incorporate female-focused initiatives as part of this growth strategy.

CHALLENGES

Barriers to Participation
Barriers that need to be addressed to improve female participation rates include societal expectations of women's role in family, perceptions that boys are generally better with computers which discourages girls to participate, discrimination and isolation during study, high cost to complete cybersecurity training courses or university study, trouble gaining promotions to senior and leadership roles, less visibility for aspiring professionals to see role models, bias hiring practices.

Limited Female-Focused Education and Training Initiatives
The market assessment of the current cybersecurity skills base in each of the five research focus countries found an absence of gender-based initiatives to increase women's access to higher education, and incentive gaps in the public and private sector with significant gaps in female-focused and gender-based initiatives.

The Need for Scale and Validation to address Gaps in the Education and Training Market
An assessment of the gap between the anticipated skill requirements and current skills and training capability and capacity across the five research focus countries found a limited offer in cybersecurity education and training, gaps in education and training for senior roles, and narrow market access for women.

RECOMMENDATIONS

Recommendations for Capacity Building Intervention Design Strategies

R1 - Interventions that Pursue an Ecosystem Approach
When developing capacity building interventions focused on increasing the participation of women in the cybersecurity workforce, it is important to consider the full ecosystem (illustrated below) in which such interventions will be deployed and the outcomes such interventions are expected to deliver.

R2 - Interventions that Incorporate a Gender-Sensitive Dimension Within Digital Development
In light of the increased investment in digital development initiatives, it is important to utilize all opportunities for promoting a gender-sensitive approach in such initiatives and ensure they include components addressing the digital literacy and cybersecurity skills gaps through relevant education, skilling, reskilling, and upskilling activities that are responsive to the needs of women and girls.

R3 - Interventions that Amplify Gender-Responsive Cybersecurity Capacity Building within the National Development Context
It is often the case that cyber capacity building interventions are pursued without a deliberate connection with the broader national development agenda. Yet, promoting the participation of women in the cybersecurity sector requires an understanding of a complexity of issues that lie at the intersection of the empowerment of women and girls, the national digital transformation journey, and the education and employment environment. This means that there is both an opportunity and a necessity to consider a systematic integration of gender-responsive approaches in cybersecurity and digital transformation actions as part of overall development objectives to deliver more equitable results for women and girls.

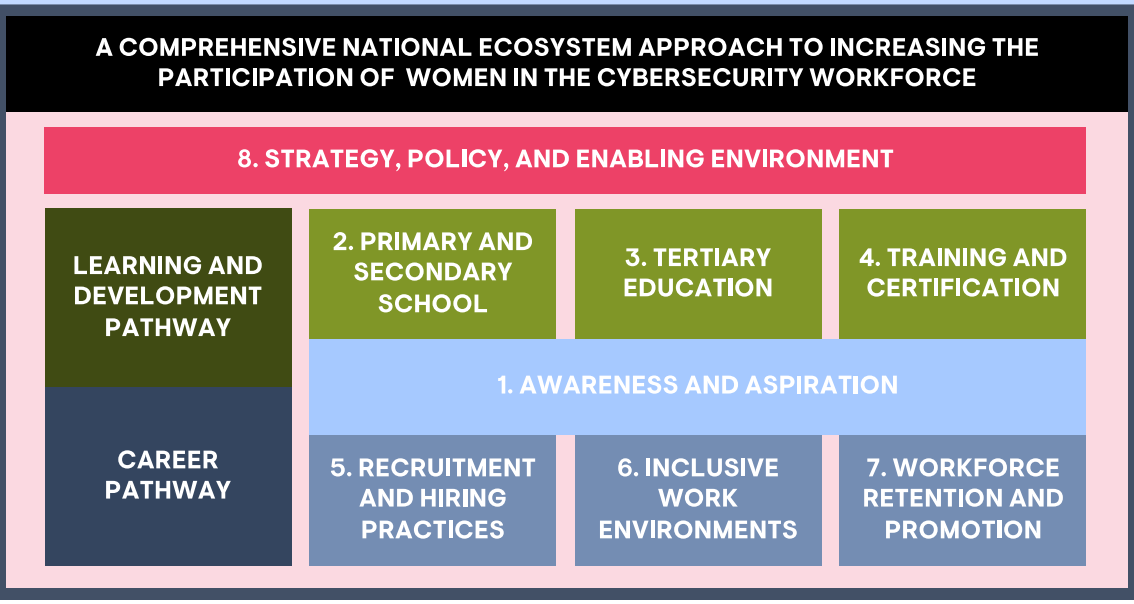
Recommendations for Capacity Building Intervention Principles and Approaches

R4 - Co-Design Interventions to Foster Sustainable, Locally-led Change
It is necessary to consider how to support co-created and locally-led interventions that build on local knowledge, capacity, and expertise and integrate collaborative efforts that address the context-specific barriers that women face in accessing and pursuing cybersecurity education and workforce opportunities.

R5 - Pursue Public-Private Partnerships and Whole-of-Society Approaches
Pursuing a whole-of-society approach that leverages the investment and expertise of government, the private sector, civil society, academia, and the research community is a starting point for all workforce initiatives which need to be informed by the local context and the gender specificities.

R6 - Balance between Short-Term and Longer-Term Intervention Approaches
When building and shaping a national workforce pipeline, there is a need to balance investments on both immediate needs and changes through targeted shorter-term interventions as well as investing in longer-term changes that will impact whole cohorts of women over time.

R7 – Account for the impact of broader systemic barriers to women's participation the Cybersecurity workforce
The design of capacity building interventions need to take into account the broader systemic barriers to women's participation in education and training and the workforce that will influence their ability to pursue cybersecurity as a profession.



Introduction

Background

This report compiles the research findings from the Women's Participation in Southeast Asia's Cybersecurity Sector project which was completed to understand the cybersecurity workforce in Cambodia, Indonesia, Laos, Mongolia and Thailand, identify gaps in the workforce to equip these five countries with the cybersecurity requirements of the future, and understand women's participation in the sector across these five geographies.

The research has also been completed in support the ITU's Women in Cyber (WiC) Mentorship Asia-Pacific Programme and to lay the foundations for future iterations of the Programme through data driven targeted capacity and skills development.

Approach



This report is the final in a multi-step project and is broken down into five key chapters as follows:

Chapter 1: Strategic Drivers
Chapter 1 describes activities and capabilities across the five focus countries which are either already planned or which are likely to be required in the next five years to mitigate risks or build maturity alongside the main existing, planned or anticipated regulatory drivers.

Chapter 2: Participation of Women in the Cybersecurity Workforce
Chapter 2 presents insights on the current cybersecurity workforce context and the participation of women in the cybersecurity workforce in the Southeast Asian region. It explores topics including understanding the current situation and initiatives, identifying barriers that need to be addressed to improve female participation rates, and the different opportunities that could be explored to close the gap.

Chapter 3: Future Workforce Assessment
This chapter presents a high-level assessment of the future workforce requirements of the five research focus countries based on the nine strategic drivers identified and defined in the Strategic Drivers chapter. This future workforce assessment extrapolates the technical cybersecurity roles and additional skills that will be required as a priority for the five research focus countries to facilitate the realisation of cybersecurity capacity building targets in response to each strategic driver.

Chapter 4: Market Assessment
This chapter presents a market assessment of the current cybersecurity skills base in each of the five research focus countries organised into four categories of (i) Primary and Secondary School, (ii) Higher Education and Research, (iii) Professional Training and Certification, and (iv) Public and Executive Awareness. As part of the market assessment a brief analysis is provided for each country

on the extent to which women in cybersecurity initiatives form part of the education and training market.

Chapter 5: Gap Assessment
This chapter combines the findings from the future workforce assessment (demand-side of cybersecurity workforce ecosystem) and the market assessment (supply-side of cybersecurity workforce ecosystem) to produce an assessment to understand the gap between the anticipated skill requirements and current skills and training capability and capacity across the five research focus countries.

Key Findings and Recommendations
Informed by the insights and analysis completed in the above five chapters, this section outlines the opportunities and challenges for the participation of women in the cybersecurity workforce in the five research focus countries and provides recommendations for future capacity building programs.

Chapter 1: Strategic Drivers

Introduction

The Strategic Driver chapter describes activities and capabilities across the five focus countries which are either already planned or which are likely to be required in the next five years to mitigate risks or build maturity alongside the main existing, planned or anticipated regulatory drivers.

The Strategic Drivers' chapter takes a high-level look of the cybersecurity environment in each country which will then be used to inform the analysis of the Future Workforce Assessment to identify the technical cybersecurity functions, teams, roles, and competencies necessary to facilitate and respond to the strategic drivers. The strategic drivers' chapter considers the cybersecurity environment and workforce as a whole, and the participation of women in the cybersecurity workforce will be explored throughout future steps of the project.

Combining these insights of the broader cybersecurity environment along with the participation of women in the workforce will then guide the identification of the different opportunities for women in cybersecurity to play an active part in the achievement of a prosperous and secure future.

Methodology

Data Collection

A combination of complimentary data collection exercises was undertaken to understand the various forces driving the need for cybersecurity skills across the five focus countries and the broader Southeast Asia region.

These included a strong reliance on secondary data sources collated via a desk-research review of key documents and information relating to national cybersecurity risks, formal and implied capacity maturity targets, and prevailing and planned legislation, regulation, and standards. Sources are detailed in the footnotes and include a range of official government publications, industry and research reports, media articles, and other publicly available data and statistics.

Findings from the desk-research review have been supplemented by responses gathered via a questionnaire distributed to government (Question Set 1) and non-government (Question Set 2) representatives to capture insights into country and regional level activities and capabilities. The questionnaire is detailed in Annex A.

Research Participants

Representatives from each of the five focus countries were invited to complete the questionnaire. These included a combination of government and non-government stakeholders from each country across various sectors and societal areas including:

- government ministries and cybersecurity agencies
- critical national infrastructure and industry
- education and training; and
- civil society and non-government organisations (NGOs)

Details of the questionnaire response profile are provided in Annex A.

Research Limitations

This research relied on a combination of purposive and convenience sampling and the findings in this chapter are not presented as a representative sample or complete analysis of the cybersecurity environment in each country. In addition, a limited research window resulted in a lower than anticipated questionnaire response rate, leading to a reliance on secondary sources to inform the majority of the analysis.

This research was not intended to be and should not be taken as a comprehensive assessment of the cybersecurity environment and forecast for each country, rather it provides an indicative representation of the strategic drivers that influence the need for future technical cybersecurity skills and workforce requirements to realise the digital development and security aspirations of each country.

Analysis of Strategic Drivers

Analysis of the research findings identified nine strategic driver thematic areas that capture the key forces that are likely to drive a need for technical cybersecurity skills in five research focus countries and Southeast Asia region in the future including:

1. Principal National Cybersecurity Risks
2. Digital Transformation
3. Legislation and Regulation
4. Critical National Infrastructure
5. National Security and Criminal Justice System
6. Incident Response
7. Security Standards and Controls
8. National and Regional Cooperation
9. Research and Development

For each topic, a definition of each strategic driver is presented as well as insights into recent related developments and plans at the Southeast Asia level to provide regional context. This is then followed by specific examples of related activity to provide an indicative insight into the cybersecurity situation for each of the five focus countries.

Principal National Cybersecurity Risks

The United States National Institute of Standards and Technology (NIST)[2] defines Cybersecurity Risk as an effect of uncertainty on or within information and technology. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation.

Southeast Asia Context
In 2021, INTERPOL published an ASEAN Cyberthreat Assessment[3] and noted the ASEAN regions:

"Increasing reliance on the Internet has created a large number of security threats that can cause immense damage. It impedes trust and resilience in the digital economy, which will prevent the region from realizing its full digital potential if nothing is done."

The chapter identified prominent cyberthreats in 2020 and beyond facing the ASEAN region which included:

- Business E-mail Compromise campaigns
- Phishing
- Ransomware
- E-commerce data interception
- Crimeware-as-a-Service (CaaS)
- Cyber scams.
- Crypto jacking

[2] https://csrc.nist.gov/glossary/term/cybersecurity_risk#:~:text=Cybersecurity%20risks%20relate%20to%20the,individuals%2C%20other%20organizations%2C%20and%20the

[3] https://www.interpol.int/content/download/16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf

Country-Level Risks

Examples of country-level cybersecurity risks are presented below and provide an indicative insight into the cybersecurity situation for each country that will influence the need for certain cybersecurity skills to respond to and mitigate such risks.

Country	Strategic Driver Insights
Cambodia	The Cambodia Digital Government Policy 2022-2035[4] noted that the main targets of attacks from hackers are the digital infrastructure, mobile networks, key infrastructures, websites of ministries and institutions, other media networks, and digital banking operating systems that make them inoperable throughout the country.
Indonesia	A 2021 Threats Landscape Report[5] details that Indonesia is a prime target for nation-state sponsored actors as well as financially motivated ransomware gangs and noted that dark web threats are on the rise. Indonesia's National Security Operations Centre recorded a five-fold increase in cyber-attacks in first of half of 2019 to the first half of 2020 with the most common attacks being Trojan related activities followed by information gathering and web application-related attacks.[6]
Laos	In 2019 Officials from the Lao Government completed a three-day training course on darknet investigations and countering terrorist operations online as a part of UNODC's Global Programme on Cybercrime. This was in response to the challenges presented with the rapid economic development and the expansion of internet connectivity.[7]
Mongolia	As Mongolia's internet penetration has grown, so have the frequency of certain cybercrimes, with credit card fraud, phishing, and e-mail spam emerging as growing risks.[8] The need to protect and prepare Mongolian Critical Infrastructure to respond to terrorist cyber-attacks was highlighted during a 2021 national workshop run by the United Nations Counter-Terrorism Centre (UNCCT) of the United Nations Office of Counter-Terrorism (UNOCT).[9]
Thailand	A media report in 2022 found that among Thai firms attacked, the top three intrusions were malware, ransomware, and hackers. The article details that Thai organisations face challenges using multiple OT security tools and that Industrial systems have become a significant risk factor as these environments were traditionally air-gapped from IT and corporate networks, but now these two infrastructures are becoming universally integrated.[10] The National Security Policy and Plan (2019-2022) acknowledges the shifting contexts that create new forms of national security threats that include the threats from changes in global economic, social and political situation, including threats from technological development and cyber interconnectivity that link the infrastructure, transportation, economic and financial systems together.[11]

4 https://asset.cambodia.gov.kh/mptc/media/Cambodia_Digital_Government_Policy_2022_2035_English.pdf

5 https://socradar.io/wp-content/uploads/2021/10/2021-Indonesia-Threat-Landscape-Report.pdf

6 https://policy-futures.centre.uq.edu.au/files/9577/Policy%20Futures_Cyber%20Security%20Indo%20Pacific_May21.pdf

7 https://www.unodc.org/roseap/en/laopdr/2019/11/cyber-crime/story.html

8 https://www.adb.org/sites/default/files/project-documents/55211/55211-001-tar-en.pdf

9 https://www.un.org/counterterrorism/events/protecting-national-critical-infrastructure-from-terrorists-cyber-attacks-mongolia

10 https://www.bangkokpost.com/tech/2386643/cyberthreats-on-the-up-at-thai-companies

11 https://www.nsc.go.th/wp-content/uploads/2020/05/The-National-Security-Policy-and-Plan2019-%E2%80%93-2022.pdf

Digital Transformation

The World Bank[12] defines digital transformation using an ecosystem approach consisting of five elements including (i) Digital infrastructure (fixed and mobile broadband, fibre-optic cables, etc.); (ii) Digital financial services and digital identification; (iii) Digital innovation and entrepreneurship; (iv) Digital platforms, including e-commerce and e-government; and (v) Digital literacy and skills.

Southeast Asia Context

Published in 2021, the ASEAN Digital Masterplan 2025[13] outlines a vision for the region positioning 'ASEAN as a leading digital community and economic bloc, powered by secure and transformative digital services, technologies and ecosystem.'
This vision is expected to be achieved through the realization of eight desired outcomes:

1. Actions of ADM 2025 prioritised to speed ASEAN's recovery from COVID-19
2. Increase in the quality and coverage of fixed and mobile broadband infrastructure
3. The delivery of trusted digital services and the prevention of consumer harm
4. A sustainable competitive market for the supply of digital services
5. Increase in the quality and use of e-government services
6. Digital services to connect business and to facilitate cross border trade
7. Increased capability for business and people to participate in the digital economy
8. A digitally inclusive society in ASEAN

Country-Level Activity

Examples of country-level planned, and ongoing digital transformation activity are presented below and provide an indicative insight into the digital development journey for each country and the cybersecurity skills that will be required to facilitate and secure such development.

Country	Strategic Driver Insights
Cambodia	The Cambodia Digital Government Policy 2022-2035[14] outlines a vision to "establish a digital government to improve the citizens' quality of life and build their trust through better public service provision". This vision will be achieved through four strategic goals including to (i) promote the development of digital government infrastructure, (ii) build digital governance and create digital public services, (iii) digital capacity building and innovation, and (iv) to promote cooperation and partnerships between public and private sectors. The Cambodia Digital Economy and Society Policy Framework 2021-2035[15] outlines a vision of "building a vibrant digital economy and society by laying the foundations to promote digital adoption and transformation in all social actors including the state, citizens, and businesses, to accelerate new economic growth and promote social welfare in the new normal". This vision will be achieved through five main goals including (i) developing infrastructures, (ii) building reliability and confidence in digital, (iii) building

[12] https://www.worldbank.org/en/topic/digitaldevelopment/overview#2
[13] https://asean.org/wp-content/uploads/2021/09/ASEAN-Digital-Masterplan-EDITED.pdf
[14] https://asset.cambodia.gov.kh/mptc/media/Cambodia_Digital_Government_Policy_2022_2035_English.pdf
[15] https://mef.gov.kh/download-counter?post=7116

	digital citizens, (iv) building digital government, (v) enabling digital businesses. The Pentagonal Strategy Pentagon 5 – Development of Digital Economy and Society, under Human Resource and Capacity Development, has Side 1.7 "Building human capital with digital skills through modernizing and finetuning education curricula and digital training programs" and Side 1.8 "Continuing to promote digital literacy among citizens, including the inclusion of basic digital skills in education curricula and provision of training programs on digital skills in various sections."[16]
Indonesia	The Indonesian Ministry of Communications and Informatics is working on accelerating national digital transformation by outlining five priorities including to (i) accelerate the development of digital infrastructure, (ii) perform radio spectrum re-farming and the development of 5G technology, (iii) initiate comprehensive and sustainable human resource development in the digital sector, (iv) prepare a digital transformation roadmap in strategic sectors, such as the government sector, public services, social welfare support, education, health, trade, industry, and broadcasting, and (v) completion of primary legislation to support the digital ecosystem.[17] Through the Making Indonesia 4.0 programme launched in April 2018, the Indonesian government wants to raise Indonesia's competitiveness in the Industry 4.0 era by utilising the power of disruptive technologies to considerably boost national manufacturing performance and productivity.[18]
Laos	A 2022 UNDP Digital Maturity Assessment of Lao PDR[19] provides details of the Lao PDR National Digital Economy Vision (2021-2040) which has the overall goal to use digital technologies and innovations as key tools to develop production innovations, distribution, marketing and digital economy services that will contribute to comprehensive national social and economic development and prepare the nation to graduate from least developing country status. To reach this vision, the National Digital Economy Strategy (2021-2030) details eight points including (i) Develop Legislation, (ii) Develop infrastructure, (iii) Develop platforms, (iv) Develop human resources, (v) Create products and services, (vi) Ensure cyber safety in relation to digital technology, (vii) Apply digital technologies, and (viii) Cooperate with national and international development partners. A 2022 report from the World Bank on 'Positioning the Lao PDR for a digital future'[20] details that the Government of the Lao PDR has articulated a vision for the digital economy to grow from the current level of 3 percent to 10 percent of GDP by 2040. The report notes that to realize this vision, Laos'

[16] https://mfaic.gov.kh/files/uploads/1XK1LW4MCTK9/EN%20PENTAGONAL%20STRATEGY%20-%20PHASE%20I.pdf

[17] https://www.eria.org/uploads/media/Books/2022-Accelerating-Digital-Transformation-Indonesia/Accelerating-Digital-Transformation-Indonesia-rev3.pdf

[18] https://www.eria.org/uploads/media/Books/2022-Accelerating-Digital-Transformation-Indonesia/Accelerating-Digital-Transformation-Indonesia-rev3.pdf

[19] https://www.undp.org/laopdr/publications/digital-maturity-assesment-lao-pdr

[20] https://thedocs.worldbank.org/en/doc/c01714a0bc2ca257bdfe8f3f75a64adc-0070062022/original/Positioning-The-Lao-PDR-for-a-Digital-Future-11-10-22.pdf

	digital transformation will need to permeate all sectors of the economy. Examples of this incudes enabling more widespread access to high-speed internet, E-commerce platforms to generate inclusive growth in rural areas, and secure digital payments. In May 2023, Lao Prime Minister Sonexay Siphandone addressed the 'Ministerial Level Conference on Blockchain 4.0 Development for Digital Economy Development in Laos' and called for intensive action to develop three digital pillars – a digital economy, government and community. Technologies including blockchain, artificial intelligence (AI), high speed Internet, Internet of Things (IoT), big data, cloud computing, E-wallet, E-transactions, E-payments, and virtual and augmented reality will bring about new opportunities and services to drive rapid changes and spur fast progress in socio-economic development and governance.[21]
Mongolia	Mongolia's long-term policy document "Vision - 2050" and the government's 2021-2024 action program set the goal of making national science, technology and innovation with international competitiveness one of the economic priorities. In the framework, six strategic goals were approved: (i) digital infrastructure, (ii) e-government, (iii) information security, (iv) digital literacy, (v) innovation production, and (vi) national development accelerator.[22] The government adopted the New Recovery Policy, a 10-year medium-term target plan, in December 2021 and its priorities include (i) restoring public sector productivity, which requires government services to be digitalized; and (ii) introducing advanced technology, blockchain, and artificial intelligence to spur an industrial recovery and align Mongolia with emerging economy trends.[23] Since its launch in 2020, the e-Mongolia platform has connected 656 services from 61 government agencies. The government plans to digitalize 1,200 licensing services by the end of 2022 and 90% of government services by 2024.[24] In June 2022, The World Bank[25] approved a credit of $40.7 million to help Mongolia improve online public services to citizens and businesses, boost digital skills training, and increase digital-enabled jobs.
Thailand	The Thailand Digital Government Development Plan 2023-2027[26] outlines a vision that "Government services are convenient, transparent, modern and meet the needs of the people." The plan specifies four development strategies in line with this vision consisting of (i) Raise the level of government digital transformation for flexible, agile management and

[21] https://kpl.gov.la/En/detail.aspx?id=73403

[22] Unofficial Translation taken from: https://mddc.gov.mn/eng/%d1%81%d1%82%d1%80%d0%b0%d1%82%d0%b5%d0%b3%d0%b8%d0%b9%d0%bd-%d0%b7%d0%be%d1%80%d0%b8%d0%bb%d0%b3%d0%be/

[23] https://www.adb.org/sites/default/files/project-documents/55211/55211-001-tar-en.pdf

[24] https://www.adb.org/sites/default/files/project-documents/55211/55211-001-tar-en.pdf

[25] https://www.worldbank.org/en/news/press-release/2022/06/06/mongolia-new-project-helps-the-government-go-digital-and-grow-the-economy

[26] Unofficial Translation from: https://www.dga.or.th/policy-standard/policy-regulation/dga-019/dga-027/dg-plan-2566-2570/

	expanding to local government agencies, (ii) Develop services that are convenient and easy to access, (iii) Creating added value and facilitating the business sector, (iv) Promote public participation and disclose information open to the public sector.

Legislation and Regulation

Cybersecurity legislation and regulation includes a range of provisions related to cybersecurity and cybercrime. This can include a range of areas including but not limited to substantive law criminal offences to procedural laws, civil-and-criminal liabilities, breach notification and vulnerability disclosure, data protection, child protection online, consumer protection and intellectual property.[27]

Convention on Cybercrime[28]

The Convention on Cybercrime, known as the 'Budapest Convention', is considered the leading international instrument focused on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child sexual abuse material and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

Southeast Asia Context

The ASEAN Cybersecurity Cooperation Strategy (2021-2025)[29] details a range of recently completed cybersecurity capacity building initiatives in the region. This included 'Sharing of Information on National Laws, Policies, Best Practices and Strategies as well as Rules and Regulations' as part of the ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies. Building on this, the ASEAN Digital Masterplan 2025[30] outlines a range of Enabling Actions (EA) that will impact the cybersecurity legislative and regulatory environments of countries in the region including:

- EA3.3: Identify improvements in legal and regulatory measures on the management of protection of data and other data-related activities that could be harmful.
- EA3.5: Promote consumer protection and rights in relation to e-commerce.
- EA4.1: Continue to identify opportunities to harmonise digital regulation to facilitate cross-border data flows.
- EA4.2: Deepen collaboration between ICT and competition regulatory authorities across ASEAN on the ICT sector and digital economy.
- EA4.3: Monitor developments in regulation of digital platforms in other jurisdictions.

Country-Level Activity

Examples of country-level planned, and ongoing legislation and regulation activity are presented below and provide an indicative insight into the evolving legislative and regulatory environment for each country and the cybersecurity skills that will be required to facilitate and ensure compliance with such changes.

[27] https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

[28] https://www.coe.int/en/web/cybercrime/the-budapest-convention

[29] https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

[30] https://asean.org/wp-content/uploads/2021/09/ASEAN-Digital-Masterplan-EDITED.pdf

Country	Strategic Driver Insights
Cambodia	The Cambodia Digital Government Policy 2022-2035[31] second strategic goal to build digital governance and create digital public services includes strategy 5 that has a focus on the creation and improvement of the legislative frameworks and relevant regulations. The Cambodia Digital Economy and Society Policy Framework 2021-2035[32] acknowledges the need to address limitations with Cambodia's legal and institutional framework for supporting and ensuring digital security and safety. It identifies key areas of priority including data protection and privacy, a law on electronic transactions, a law on public information, and law on cybercrime. A final draft of a cybercrime law was submitted to the Council of Ministers in late 2022 and includes provisions on a range of areas including the integrity of the use, management and security of computer systems, devices and databases, and to crack down on cybercrime to protect security, public order and people's rights and freedoms.[33] In late 2019, Cambodia adopted the E-Commerce Law and a Consumer Protection Law. On 1 March 2024, Cambodia issued a sub-decree on the Digital Security Committee to lead and support digital cybersecurity to protect the country from cyberattacks and defend against national threats in line with the digital economy and society policy framework 2021-2035.
Indonesia	A comprehensive draft cyber security bill—the Cyber Security and Resilience Bill was originally included in the Indonesian parliament's priority legislative agenda for 2020, but was delayed due to COVID-19 priorities. [34] In 2022, Indonesia enacted its first Personal Data Protection Law which states the types of legal basis for obtaining and processing personal data and sets out strict criminal and administrative sanctions for those that break the provisions under the law.[35] Indonesia recently released new cybersecurity rules for the financial sector. Developed by the Financial Services Authority are Indonesia's first dedicated cybersecurity rules specifically for the financial sector and cover a range of topics including risk assessments, risk management, data protection, incident response planning, and employee capacity.[36]

[31] https://asset.cambodia.gov.kh/mptc/media/Cambodia_Digital_Government_Policy_2022_2035_English.pdf

[32] https://mef.gov.kh/download-counter?post=7116

[33] https://www.phnompenhpost.com/national/draft-cybercrime-law-nearing-completion

[34] https://policy-futures.centre.uq.edu.au/files/9577/Policy%20Futures_Cyber%20Security%20Indo%20Pacific_May21.pdf

[35] https://www.aseanbriefing.com/news/indonesia-enacts-first-personal-data-protection-law-key-compliance-requirements/

[36] https://www.aseanbriefing.com/news/new-cybersecurity-rules-for-financial-institutions-in-indonesia/

Laos	A 2022 report from the World Bank on 'Positioning the Lao PDR for a digital future'[37] details recommendations related to cyber legislation and regulation that will support Lao PDR in realizing its vision for a digital future. These recommendations include improving alignment of substantive provisions (cybercrime) with international good practice frameworks, adopting a data protection law, updating consumer protection and strengthening related regulatory capacity and enforcement mechanisms. A 2022 UNDP Digital Maturity Assessment of Lao PDR[38] found that the Government of Lao PDR has developed basic legislation for ICT, digital payments, transactions and trade to support the digital government initiative as well as laws related to cybersecurity and data protection. The report notes The National Digital Economy Strategy (2021-2030) includes a key point to develop legislation which will reassess existing laws and improve and develop new legislation to promote and create favourable environments for digital economy development.
Mongolia	The Mongolia National Cyber Security Strategy[39] includes activities listed under 3.1.1. to strengthen the legal framework for cyber security which covers topics such as mutual exchange of information, regulations for cybersecurity standards, improvement of the legal framework for combating violations of human rights, spreading false information and such violations in the cyber environment, child protection in the cyber environment, fight against cyber terrorism and crime. The Law of Mongolia on Cyber Security 2021 defines its purpose to regulate relations pertaining to establishing the system, principles, and legal framework in ensuring cyber security, and ensuring the safety, confidentiality, and accessibility of information within cyberspace and cyber environments.[40] New laws enacted by Parliament in December 2021 will advance digitalization and cover areas such as the transparency of public information, protection of personal information, use of digital signatures, provision of virtual asset services, and cybersecurity.[41] In June 2022, The World Bank[42] approved a credit of $40.7 million for The Smart Government II Project which includes aims to improve Mongolia's legal and regulatory environment for building trust and cybersecurity in the use of digital technologies.
Thailand	The Cyber Security Act B.E. 2562 (2019) contains a range of provisions developed to efficiently protect cybersecurity and to establish approaches to protect, cope with, and mitigate the risk of Cyber Threats which affect the

[37] https://thedocs.worldbank.org/en/doc/c01714a0bc2ca257bdfe8f3f75a64adc-0070062022/original/Positioning-The-Lao-PDR-for-a-Digital-Future-11-10-22.pdf

[38] https://www.undp.org/laopdr/publications/digital-maturity-assesment-lao-pdr

[39] Unofficial Translation taken from: https://legalinfo.mn/mn/detail?lawId=16532522791411&showType=1

[40] Unofficial Translation taken from: https://legalinfo.mn/en/edtl/16531350476261

[41] https://www.adb.org/sites/default/files/project-documents/55211/55211-001-tar-en.pdf

[42] https://www.worldbank.org/en/news/press-release/2022/06/06/mongolia-new-project-helps-the-government-go-digital-and-grow-the-economy

	national security and public order.[43] Thailand has been actively promoting and formulating secondary legislation in alignment with the Cybersecurity Act of 2019. This is to serve as a framework, setting standards, guidelines, and practices for preventing, responding to, and mitigating risks associated with cyber threats. Furthermore, policies and operational plans addressing cybersecurity have been established for the period 2022 to 2027. The Personal Data Protection Act B.E. 2562 (2019) of Thailand (PDPA) became effective on 1 June 2022.[44]

[43] https://cyrilla.org/es/entity/4nywjpircms?page=1

[44] https://www.nortonrosefulbright.com/en/knowledge/publications/e29d223d/overview-of-thailand-personal-dataprotection-act-be2562-2019#:~:text=by%20the%20Committee.-,General%20protections,of%20the%20prescribed%20exceptions%20applies

Critical National Infrastructure

Critical National infrastructure (CNI)[45] is defined as "those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in: a) Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or b) Significant impact on national security, national defence, or the functioning of the state."

Southeast Asia Context

The ASEAN Cybersecurity Cooperation Strategy (2021-2025)[46] includes Critical Information Infrastructure (CII) as a key component of Advancing Cyber Readiness Cooperation as detailed in Dimension 1 of the strategy, and in 2020 participants in the informal ASEAN Ministerial Conference on Cybersecurity (AMCC) agreed on the urgent need to protect national and cross-border CII. This led to the proposal that the ASEAN Network Security Action Council (ANSAC) would lead the 'Development of ASEAN Critical Information Infrastructure Protection (CIIP) Coordination Framework, built upon the ASEAN CIIP Framework (2020)'. In addition, the ASEAN Digital Masterplan[47] also acknowledges Critical Information Infrastructure Protection (CIIP) as a core strategic issue and highlights in EA3.2 four essential industry sectors of finance, healthcare, education and government as focus points for developing trust and security frameworks for these industries, including secure certification and specialist cybersecurity incident response capabilities.

Country-Level Activity

Examples of country-level planned, and ongoing Critical National Infrastructure activity are presented below and provide an indicative insight into the requirements and demands on critical national infrastructure assets and organizations, and the cybersecurity skills that will be required to secure and mitigate cybersecurity risks and threats to their operation.

Country	Strategic Driver Insights
Cambodia	The Cambodia Digital Government Policy 2022-2035[48] Strategic Goal 1: Promoting the development of digital government infrastructure includes Strategy 3 Building and strengthening digital security infrastructure. This strategy details the aim to protect digital infrastructure and ensure high security and safety on management, operation, and use of digital systems. One of the priority actions for this strategy includes strengthening the management and protection system for the national information infrastructure. The Cambodia Digital Economy and Society Policy Framework 2021-2035[49] identifies focus areas for the Royal Government in building digital infrastructure on three aspects: digital connectivity, Financial Technology (FinTech) infrastructure and digital payment systems, and logistics and last-mile delivery.
Indonesia	Article 3 of the Presidential Regulation Number 82 of 2022 on Protection for Vital Information Infrastructure (IIV) details that the scope of IIV protection

[45] https://www.cpni.gov.uk/critical-national-infrastructure-0

[46] https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

[47] https://asean.org/wp-content/uploads/2021/09/ASEAN-Digital-Masterplan-EDITED.pdf

[48] https://asset.cambodia.gov.kh/mptc/media/Cambodia_Digital_Government_Policy_2022_2035_English.pdf

[49] https://mef.gov.kh/download-counter?post=7116

	includes identification of IIV sector and IIV, protection for IIV, fostering and monitoring of IIV protection, and coordination of IIV protection. Strategic sectors included as IIV and the ministries/institutions responsible for those sectors are: (i) Government administration sector by the State Cyber and Encryption Agency (BSSN); (ii) Energy and mineral resources sector (ESDM) by Ministry of Energy and Mineral Resources Ministry; (iii) Transportation sector by Ministry of Transportation; (iv) Financial sector by the authority that manages and monitors financial sector; (v) Health sector by Ministry of Health; (vi) Information technology and communication sector by Ministry of Communication and Informatics; (vii) Food sector by Ministry of Agriculture; and (viii) Defense sector by Ministry of Defense.
Laos	A 2022 report from the World Bank on 'Positioning the Lao PDR for a digital future'[50] details recommendations related to critical infrastructure that will support Lao PDR in realizing its vision for a digital future. This includes guidance to develop a national cybersecurity strategy that lays out how to secure critical infrastructure and technologies.
Mongolia	The Mongolia National Cyber Security Strategy[51] includes activities listed under 2.2.2. to ensure cyber security of organizations with critical information infrastructure and covers topics such as risk management systems in public and private organizations with critical information infrastructure, establishing a laboratory for checking and certifying information, communication equipment and information systems used in organizations with state and critical information infrastructure, and a crisis management system in organizations with critical information infrastructure. The Mongolia National Cyber Security Strategy[52] includes activities listed under 2.2.2. to ensure cyber security of organizations with critical information infrastructure and covers topics such as risk management systems in public and private organizations with critical information infrastructure, establishing a laboratory for checking and certifying information, communication equipment and information systems used in organizations with state and critical information infrastructure, and a crisis management system in organizations with critical information infrastructure.
Thailand	The Cyber Security Act B.E. 2562 (2019)[53] contains a range of provisions related to Critical Information Infrastructure. This includes Section 49 which identifies key sectors that includes organisations of Critical Information Infrastructure which comprises (i) national security, (ii) substantive public service, (iii) banking and finance, (iv) information technology and telecommunications, (v) transportation and logistics, (vi) energy and public utilities, (vii) public health, and (viii) others as prescribed by the Committee. The Act includes other sections which detail requirements for organisations of Critical Information Infrastructure such as conducting risk assessments (Section 54), Incident Response Mechanisms (Section 56), Reporting Mechanisms (Section 57).

[50] https://thedocs.worldbank.org/en/doc/c01714a0bc2ca257bdfe8f3f75a64adc-0070062022/original/Positioning-The-Lao-PDR-for-a-Digital-Future-11-10-22.pdf

[51] Unofficial Translation taken from: https://legalinfo.mn/mn/detail?lawId=16532522791411&showType=1

[52] Unofficial Translation taken from: https://legalinfo.mn/en/edtl/16531350476261

[53] https://cyrilla.org/es/entity/4nywjpircms?page=1

	The National Security Policy and Plan (2019-2022)[54] includes a strategic goal that Thailand is safe, secured and well-prepared for the handling of cyber threats. One indicator for this goal is to establish an effective cyber security system for the protection of the government's electronics data and key cyber infrastructures.

National Security and Criminal Justice System

Capacity to respond to cyber threats is important for countries to defend their national security and create a safe environment for the use of ICTs throughout society. National security actors include key government security agencies and defense-force entities tasked with protecting the cyber environment and interests of the country. Criminal justice sector actors include law enforcement, prosecutors, and courts involved in the investigation and prosecution of cybercrime cases and play leading roles in the enforcement of capabilities of a country's cybercrime legislation.[55]

Southeast Asia Context

National Security

For national security and defense the ADMM Cybersecurity and Information Centre of Excellence (ACICE)[56] was approved by the 15th ASEAN Defence Ministers' Meeting (ADMM) in 2021. ACIC was set up to 'focus on confidence-building measures, enhancing information-sharing, and capacity building among ASEAN defence establishments. The ACICE aims to enhance multilateral cooperation among ASEAN defence establishments against cyberattacks, disinformation and misinformation, for the region's collective peace and security'.

Criminal Justice System

The ASEAN Cybersecurity Cooperation Strategy (2021-2025)[57] details a range of recently completed cybersecurity capacity building initiatives in the region. This included a 'Workshop on Countering the Use of ICTs for Criminal Purposes' as part of the ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies. Furthermore, in 2018 INTERPOL established the ASEAN Cybercrime Operations Desk[58] (formerly the ASEAN Cyber Capability Desk) to support countries in the region to tackle cybercrime using intelligence development, investigative support, operational coordination and through connecting law enforcement authorities with the private sector and other partners who can provide support.

ASEAN plan of action in combating transnational crime (2016-2025)[59] outlines a commitment to combating transnational crimes under the frameworks of the ASEAN Ministerial Meeting on Transnational Crime (AMMTC) and the Senior Officials Meeting on Transnational Crime (SOMTC) and includes Cybercrime as one of eight focus areas. The SOMTC Working Group on Cybercrime[60] was established in 2013 in Vientiane, Lao PDR to think through practical cooperation in combating cybercrime among ASEAN Member States as well as between ASEAN and its Dialogue Partners. Since its first Meeting in 2014, it has been convened six times, with the most recent held in 2019 and has

[54] https://www.nsc.go.th/wp-content/uploads/2020/05/The-National-Security-Policy-and-Plan2019-%E2%80%93-2022.pdf
[55] https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf
[56] https://www.acice-asean.org/aboutacice/
[57] https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf
[58] https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/ASEAN-Cybercrime-Operations-Desk
[59] https://asean.org/wp-content/uploads/2021/01/ASEAN-Plan-of-Action-in-Combating-TC_Adopted-by-11th-AMMTC-on-20Sept17-1.pdf
[60] https://asean.org/senior-officials-meeting-on-transnational-crime-somtc/

been postponed since 2020 indefinitely due to COVID-19. The Terms of Reference[61] for the working group outlines it scope including:

- To facilitate information sharing on cybercrime related issues such as trends, best practices, and new techniques and tools;
- To establish regular points of contact for cybercrime cooperation;
- To develop capability building and training initiatives;
- To identify critical areas for collaboration within the ASEAN Member States and with Dialogue Partners, on cybercrime; and
- To explore possible collaboration with strategic private sector partners.

Lastly, the 2017 ASEAN Declaration to Prevent and Combat Cybercrime[62] resolved to strengthen the commitment of ASEAN Member States to cooperate at the regional level in preventing and combating cybercrime through a range of measures some of which included:

- ENHANCE cooperation and coordination among ASEAN bodies and other relevant national agencies or organizations in dealing with cybercrime to reinforce efforts through exchanges of information, experiences and good practice;
- STRENGTHEN capacities of each ASEAN Member States in addressing cybercrime through provision of assistance to each other in the form of training and research facilities in the educational, professional, technical and administrative spheres;
- ENHANCE cooperation between ASEAN Member States and its Dialogue Partners, as well as relevant agencies and organizations at regional and international levels, such as ASEANAPOL, EUROPOL, and the INTERPOL, among others, to enhance cyberspace security, prevention and response capabilities with regard to cybercrime and cyber-related matters;
- REINFORCE ASEAN's abilities to build and enhance its capabilities to prevent and combat cybercrime by working closely with the INTERPOL Global Complex for Innovation (IGCI), including by voluntarily seconding or stationing cybercrime specialists there; and
- MONITOR AND REVIEW the implementation of this Declaration through the Lead Shepherd for consideration and adoption by the SOMTC and AMMTC, to be facilitated by the ASEAN Secretariat.

Country-Level Activity

Examples of country-level planned and ongoing national security and criminal justice system activity are presented below and provide an indicative insight into the cybersecurity skill requirements to support national security and prevention and enforcement of cybercrime cases.

Country	Strategic Driver Insights
Cambodia	Cambodia's National Defence Policy 2022[63] includes Cyber Security in Chapter 5 on National Security Protection which includes a range of strategies. Examples include establishing a legal framework for the Royal Cambodian Armed Forces (RCAF) to consider cybersecurity as a priority task, amending RCAF organizational structures to align with technological evolutions and

[61] https://asean.org/wp-content/uploads/2021/01/DOC-8-Adopted-TOR-ASEAN-Cybercrime-Working-Group-1.pdf

[62] https://asean.org/wp-content/uploads/2017/11/ASEAN-Declaration-to-Combat-Cybercrime.pdf

[63] https://dot.mod.gov.kh/wp-content/uploads/2022/05/National-Defence-Policy-English.pdf

	strengthen technical capability and modernize operation systems, software and core networks. In 2023, Cambodia requested support for the training of the Kingdom's Police Officers in the fight against cybercrime. The support will include providing advisers to formulate Cambodia's National Police policies, supporting the establishment of the Transnational Crime Team (TCT) and providing capacity building for the Kingdom's police officers. It also included assistance in building new facilities and other large-scale projects.[64]
Indonesia	In 2022 the Indonesian National Police announced the establishment of Cyber Crime Directorate in every police station throughout Indonesia.[65] The Indonesian National Police is also one of the main authorities that has a special unit for the prosecution of cybercrime in particular.[66] In 2022 the Indonesian National Armed Forces built a cyber security network in 43 work units under the Indonesian National Armed Forces. The construction of the cyber security network is to improve the cyber defense of the Indonesian National Armed Forces and anticipate various digital threats as well as to support the work of the military incident response team.[67]
Laos	A 2022 report from the World Bank on 'Positioning the Lao PDR for a digital future'[68] details recommendations related to cybercrime that will support Lao PDR in realizing its vision for a digital future. This includes guidance for Lao PDR to (i) clarify evidentiary rules for the admissibility of electronic evidence, (ii) improve due process safeguards regarding the obtention of evidence in cybercrime investigations, (iii) to support proactive efforts to strengthen institutional functions and processes to help prevent and respond to cyberattacks and make it possible for Laos to participate more effectively in international efforts to combat cybercrime. In 2019 the Lao People's Democratic Republic Police Force and the United Nations Office on Drugs and Crime (UNODC) Global Programme on Cybercrime jointly opened Laos' first Digital Forensics Laboratory. The lab will specialize in the analysis of digital evidence seized, or resulting from, criminal investigations in Laos including transnational organized crime, cybercrime and wildlife crime.[69]
Mongolia	In 2020 NATO completed a multi-year project to strengthen Mongolia's cyber defence capacity which included the establishment of a Cyber Security Centre for the Mongolian Armed Forces and the provision of specialized training and equipment.[70]

[64] https://www.phnompenhpost.com/national/cambodia-looks-australia-cybercrime-help

[65] https://inp.polri.go.id/2022/09/16/the-national-police-will-establish-cyber-crime-directorate-in-regional-police-throughout-indonesia/

[66] https://www.dataguidance.com/opinion/indonesia-cybersecurity

[67] https://www.theindonesia.id/news/2022/04/05/122627/indonesian-army-sets-cyber-unit-for-hybrid-war

[68] https://thedocs.worldbank.org/en/doc/c01714a0bc2ca257bdfe8f3f75a64adc-0070062022/original/Positioning-The-Lao-PDR-for-a-Digital-Future-11-10-22.pdf

[69] https://www.unodc.org/roseap/en/laopdr/2019/08/digital-evidence-forensics-laboratory/story.html

[70] https://www.nato.int/cps/en/natohq/news_180697.htm

	The Law of Mongolia on Cyber Security 2021[71] includes an 'Article 20 Center against attacks and violations' which includes the establishment of an Armed forces center against cyber-attacks and violations. Article 23 outlines the functions of the Armed forces centre including preventing and responding to defence directed cyber-attacks, supporting prevention of foreign cyber-attacks, cooperation with foreign countries and international counterpart organizations on ensuring cyber security, and to verify and certify and issue conclusions on the technical equipment and software designated to ensure the cyber security in the defense sector. The Law of Mongolia on Cyber Security 2021[72] includes an 'Article 15 Police Authority' which details the cybersecurity authority of Police including to receive information on crimes related to cyber-attacks and violations, and conduct operations stipulated in the law, requisition and access information, submit recommendations, requirements, and warnings related to ensuring cyber security, operate a quantitative analytical laboratory for the purposes of fighting cyber-attacks and violations, verify equipment and software, conduct research and development work, and issue conclusions. The 2021 National Security Concept of Mongolia includes Chapter 3 on 'National Security Components and Compliance' details a commitment to develop national capacity-building on computational forensics analysis to combat cybercrime or investigate, detect and collect evidence of crimes.[73]
Thailand	Thailand has a Bureau of Technology and Cyber Crime[74] which includes duties to perform work for preventing, suppressing and investigating special crime, and for prosecuting offenders in technology and cybercrime. The Immediate Policy of the Minister of Defence (Fiscal Year 2022)[75] includes a plan for the Armed Forces to develop the capability of cyberoperation in the area of personnel, equipment knowledge base and the management system by conducting integrated collaboration with all sectors both domestically and internationally in order to effectively combat cyber threats that undermine our national security as well as support cyber security cooperation at the national level. The National Security Policy and Plan (2019-2022)[76] includes a strategy to develop a cyber operation for military purposes through cooperation with all sectors, both domestic and overseas as part of efforts to strengthen and develop national defense capability. This also includes developing the capacity of state agencies, military and civilian agencies, the police and other sectors within the country for the prevention and resolution of cyber security problems, including for the support of the digital society.

[71] Unofficial Translation taken from: https://legalinfo.mn/en/edtl/16531350476261

[72] Unofficial Translation taken from: https://legalinfo.mn/en/edtl/16531350476261

[73] https://mfa.gov.mn/en/wp-content/uploads/sites/3/2021/02/national-security-concept-of-mongolia.pdf

[74] https://www.dsi.go.th/en/Detail/DSI-Organizational-Structure#go6

[75] https://www.mod.go.th/File/PolicyMOD64en.aspx

[76] https://www.nsc.go.th/wp-content/uploads/2020/05/The-National-Security-Policy-and-Plan2019-%E2%80%93-2022.pdf

Incident Response

Incident response relates to governments and organisations capacity to identify and resolve cyber-attacks and limit potential harms and consequences of such attacks. Computer Security Incident Response Teams (CSIRT) at the sectoral, national, and regional level typically take leadership roles in organizing, coordinating, and operationalizing such incident-response capabilities.[77]

Southeast Asia Context

The ASEAN Cybersecurity Cooperation Strategy (2021-2025)[78] details that the ASEAN agreed on the establishment of an ASEAN CERT to facilitate the timely exchange of threat and attack-related information. The ASEAN CERT is expected to have a range of functions including:

- Facilitate coordination and information sharing between AMS National level CERTs
- Develop and maintain an ASEAN POC network of cybersecurity experts and organisations
- Host ASEAN cybersecurity conferences, trainings and drills for AMS national CERTs
- Facilitate and conduct regional cybersecurity exercises
- Partner with other international and regional organisations in support of ASEAN cybersecurity interests and objectives
- Develop partnerships with industry and academia
- Support AMS National CERT capacity building and best practices
- Conduct and support cybersecurity awareness campaigns

This was further emphasized in the ASEAN Digital Masterplan[79] which includes EA3.4 to achieve 'Improved coordination and cooperation for regional computer incident response teams'. This is to be achieved by expanding and extending existing coordination between individual country computer response teams and to fully establish a regional CSIRT for ASEAN. The ASEAN Regional CERT is targeted to be established in 2023/2024, following ASEAN Member States agreement on the Operational Framework this year, and the Financing Model thereafter.[80]

A 2023 report from the International Institute for Strategic Studies[81] proposes the need for identified steps towards creating an 'ASEAN cyber-emergency-response framework' and highlights the important role such an initiative could play in boosting cyber resilience in the region.

Country-Level Activity

Examples of country-level planned, and ongoing incident response activity are presented below and provide an indicative insight into the cybersecurity skill requirements to support incident response capacity and capacity to identify and respond to cybersecurity-attacks.

Country	Strategic Driver Insights
Cambodia	Cambodia has a national incident response team, the Cambodia Computer Emergency Response Team (CamCERT). CamCERT provides computer information security advice to and cooperates closely with the Cambodian

[77] https://gcscc.ox.ac.uk/cmm-2021-edition

[78] https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

[79] https://asean.org/wp-content/uploads/2021/09/ASEAN-Digital-Masterplan-EDITED.pdf

[80] https://www.csa.gov.sg/News-Events/Press-Releases/2022/establishment-of-asean-regional-computer-emergency-response-team

[81] https://www.iiss.org/research-paper/2023/06/asean-cyber-security-cooperation-towards-a-regional-emergency-response-framework/

	Government, Internet Service Providers (ISP/IX), local/international CSIRTs, as well as the Cambodian public including ICT vendors, National Security Communities, and corporate/individual users.[82] The Cambodia Digital Government Policy 2022-2035[83] acknowledges the general status of digital security in government is low and there is a lack of officials in-charge of digital security, high level of risk, and inability to timely respond when an incident occurs on the database and software systems.
Indonesia	Indonesia has a national incident response team, the Indonesia Computer Emergency Response Team (idCERT).[84] Indonesia also has the Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center (Id-SIRTII/CC) which has the mission to "Increase internet growth in Indonesia through awareness campaign efforts to safeguard technology and information systems, monitoring potential security incidents, support law enforcement, and provide technical support".[85] The Indonesian National Competency Standards (SKKNI) in the field of Cyber Security, initiated by the Directorate of HR Policy for Cyber Security and established by the Ministry of Manpower of the Republic of Indonesia, include: 1. SKKNI in the field of Security Operation Center, 2. SKKNI in the field of Information Security Audit, 3. SKKNI in the field of Cyber Security Testing, and 4. SKKNI in the field of Cryptography.[86] In addition, there are 2 SKKNI related to information security: 1. SKKNI in the field of Personal Data Protection 2. SKKNI in the field of Digital Forensics, with a subfield in Initial Handling of Electronic Evidence[87] The National Cyber Security Occupation Map (Peta Okupasi Nasional Keamanan Siber (PONKS) 2019 was crafted as a living document that can dynamically, adaptively, and flexibly evolve in response to changes.[88] This document has been updated by the PONKS Development Team of the Directorate of HR Policy for Cyber Security (KSS), expanding from its original 30 occupations to 33 occupations. This includes 14 unchanged occupations, 10 revised occupations, 9 new occupations, and 5 removed occupations. [89]
Laos	Lao PDR has a national incident response team, the Lao Computer Emergency Response Team (LaoCERT).[90]

[82] https://www.camcert.gov.kh/en/who-we-are/

[83] https://asset.cambodia.gov.kh/mptc/media/Cambodia_Digital_Government_Policy_2022_2035_English.pdf

[84] https://www.cert.or.id/

[85] https://idsirtii.or.id/en/page/vision-%26-mission.html

[86] https://skkni.kemnaker.go.id/tentang-skkni/dokumen?agency=a543995d-daef-4ccc-8753-9962b7d98968&limit=20&page=1

[87] https://skkni.kemnaker.go.id/tentang-skkni/dokumen?agency=5c4c17af-06bd-4e77-a50a-7af5de734aca&limit=20&page=1

[88] https://cloud.bssn.go.id/s/8aHmiZENZ3fx6ef

[89] https://www.bssn.go.id/wp-content/uploads/2024/07/PONKS-SKKNI-KAMSIBER.pdf

[90] http://laocert.gov.la/Home

	The 2015 Law on Prevention and Combatting Cyber Crime[91] includes 'Chapter III – Law Computer Emergency Response Center' which outlines the duties of Lao CERT which includes items such as strategic planning, regulation development, dissemination of laws, training personnel, risk assessments, receive cybercrime reports, and coordinating across sectors and foreign countries.
Mongolia	Mongolia has a national incident response team, the Mongolian Cyber Emergency Response Team / Coordination Centre (MN CERT/CC).[92] The Mongolia National Cyber Security Strategy[93] includes incident response activities such as to establish the National Center, the Public Center and the Armed Forces Center for combating cyber-attacks, establish a digital analysis laboratory for the analysis of cyber-attacks, develop basic infrastructure for exchanging information about cyber-attacks. The Law of Mongolia on Cyber Security 2021[94] includes an 'Article 20 Center against attacks and violations' with the functions of the National Centre detailed in Article 21 covering topics such as to coordinate and facilitate centers against cyber-attacks and violations nationwide, detecting, and responding to cyber-attacks, analysis of information on cyber-attacks, collaborations and exchange of information with local and international stakeholders. The Law of Mongolia on Cyber Security 2021[95] also includes 'Article 22 Public Centre' with the functions covering topics such as to detect and respond to cyber-attacks and violations directed at individuals and legal persons and restoration of the targeted information systems, conduct research and analysis on cyber-attacks, cooperate and exchange information, issue and submit recommendations regarding cyber-attacks to citizens and legal persons.
Thailand	Thailand has a national incident response team, Thailand Computer Emergency Response Team (ThaiCERT)[96] which is tasked with monitoring the risk of occurrence of Cyber Threats, follow, analyze, and process information in relation to the Cyber Threats and the alerts on the Cyber Threats. Thailand also has the Thailand Banking Sector Computer Emergency Response Team (TB-CERT) established with the approval of senior management of commercial banks in Thailand to encourage exchange of information and experiences for the overall benefit of financial institutions in Thailand in preventing cyber threats that may affect services, resources or personnel of the organization.[97]

[91] https://laocert.gov.la/ftp_upload/Cyber_Crime_Law_EnVersion.pdf

[92] https://mncert.org/#/en

[93] Unofficial Translation taken from: https://legalinfo.mn/mn/detail?lawId=16532522791411&showType=1

[94] Unofficial Translation taken from: https://legalinfo.mn/en/edtl/16531350476261

[95] Unofficial Translation taken from: https://legalinfo.mn/en/edtl/16531350476261

[96] https://www.thaicert.or.th/en/about-ncert/

[97] Unofficial Translation taken from: https://www.tba.or.th/pso-tb-cert/tb-cert/about-tb-cert/background/

Security Standards and Controls

Cybersecurity standards include international, national, and industry specific techniques and baseline requirements for cybersecurity good practice that can be implemented across public, private, and civil society sector organisations including ICT Security Standards, Standards in Procurements, and Standards for the provision of Products and Services. Security controls include physical, technological, and cryptographic security safeguards to assist organizations to mitigate the risks of cybersecurity threats with a range of internationally established cybersecurity frameworks which provide good practice guidance such as NIST and COBIT.[98]

Southeast Asia Context

The ASEAN Cybersecurity Cooperation Strategy (2021-2025)[99] includes Promoting International Cybersecurity Standards as a key component of Enhancing Trust in Cyberspace as detailed in Dimension 3 of the strategy. 'This dimension focuses on building trust through the adoption of international cybersecurity standards to secure the increased use of emerging technology' such as 5G and Internet of Things (IoT). To achieve this ASEAN intends to embark on the following initiatives:

- Development of regional cybersecurity standards for IoT.
- Development of regional cyber security policy, procedure and guideline for 5G and IoT implementation.
- Development of regional cyber security policy, procedure and guideline for SMART City implementation.
- Capacity building activities on digital infrastructure product and software security testing and certification.

In addition, the ASEAN Digital Masterplan[100] also acknowledges the importance of Cybersecurity Standards, highlighting 'Network resilience and Cyber Security standards and best practices' as a key focus point of Strategic Thrust 3 on Resilience, Trust and Security and 'Policies, regulation and standards in the digital economy' as a key focus point of Strategic Thrust 4 on Digital Policy, Regulation and Standards.

Country-Level Activity

Examples of country-level planned, and ongoing security standards and controls activity are presented below and provide an indicative insight into the cybersecurity skill requirements to support the compliance and monitoring of ICT and Cybersecurity standards and controls.

Country	Strategic Driver Insights
Cambodia	The Cambodia Digital Government Policy 2022-2035[101] acknowledges the need for cybersecurity standards and controls. An example of this in Strategy 3 details a priority action to strengthen the management and protection system for the national information infrastructure through the establishment of security procedures and the installation of technical equipment for monitoring and preventing cyberattacks in accordance with digital security standards. In addition, Strategy 5 includes a priority action to

98 https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

99 https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

100 https://asean.org/wp-content/uploads/2021/09/ASEAN-Digital-Masterplan-EDITED.pdf

101 https://asset.cambodia.gov.kh/mptc/media/Cambodia_Digital_Government_Policy_2022_2035_English.pdf

	develop digital security standards for the digital government, to define the terminology, mechanisms, technical frameworks, operation, the digital security management system, and code of conduct for monitoring digital security, for the purpose of ensuring the security and safety of its information systems. The Cambodia Digital Economy and Society Policy Framework 2021-2035[102] includes the introduction and implementation of policy measures on cybersecurity which includes the need to establish the standards, technical frameworks, and response procedures as a basis for the implementation in developing digital systems and infrastructure which are resilient against attacks. The Prakas of the Ministry of Industry, Science, Technology and Innovation in 2021 "Prakas on Cambodia Digital Standards 3 Standards" where Cambodia is set to fully accept international standards (ISO / IEC) for use in the Kingdom of Cambodia, including: - CS ISO/IEC 27000:2021 (IDT/ED 2018) - CS ISO/IEC 27001:2021 (IDT/ED 2013) - CS ISO/IEC 27002:2021 (IDT/ED 2013)[103]
Indonesia	In 2020 Indonesia's authority on cybersecurity supervision, the National Cyber and Encryption Agency (BSSN), extended the obligation to apply ISO/IEC 27001 international standard to managed information security to include electronic system providers for both public services and the private sector (Article 4 of BSSN Regulation No. 8).[104] Articles of a draft Cybersecurity Bill for Indonesia included articles that stipulated certification requirements for businesses that plan to develop cybersecurity services and products for the government procurement process and required businesses to get BSSN certifications for the products they want to offer for cybersecurity. In addition, other draft Articles required that human cybersecurity resources need to meet BSSN standards and acquire certifications from organizations accredited by BSSN.[105]
Laos	A 2022 UNDP Digital Maturity Assessment of Lao PDR[106] found a lack of a whole-of-government enterprise architecture, shortage of upgraded ICT devices, and absence of a centralized operability framework with Architecture, Standards and Interoperability the lowest-scoring focus area.

[102] https://mef.gov.kh/download-counter?post=7116

[103] https://secudemy.com/wp-content/uploads/2021/05/%E1%9E%9F%E1%9F%81%E1%9E%85%E1%9E%80%E1%9F%92%E1%9E%8F%E1%9E%B8%E1%9E%94%E1%9F%92%E1%9E%9A%E1%9E%80%E1%9E%B6%E1%9E%9F_%E1%9E%9F%E1%9F%92%E1%9E%8F%E1%9E%84%E1%9F%8B%E1%9E%8A%E1%9E%B6%E1%9E%9A_%E1%9E%8C%E1%9E%B8%E1%9E%87%E1%9E%B8%E1%9E%90%E1%9E%9B_2021.pdf

[104] https://www.dataguidance.com/opinion/indonesia-cybersecurity

[105] https://www.econstor.eu/bitstream/10419/249442/1/CIPS-PB09.pdf

[106] https://www.undp.org/laopdr/publications/digital-maturity-assesment-lao-pdr

	A 2022 report from the World Bank on 'Positioning the Lao PDR for a digital future'[107] details that within the next five years, Laos will further develop the national payments system infrastructure to increase interoperability. The payment infrastructure will be up to date, meet the needs of the industry, and observe the relevant international standards. The report also notes that there are no technical standards that lay out how government services should be built and operated and that the current computer security development plan, which is part of the Technology and Communication Plan (2021-2026), does not set specific guidelines and standards for line ministries to adhere to.
Mongolia	The Mongolia National Cyber Security Strategy[108] includes activity to establish the current and target level of cyber security and cooperate with international and foreign organizations in introducing international standards and methods. The Law of Mongolia on Cyber Security 2021[109] includes 'Article 8 Cybersecurity Risk Assessment' and 'Article 9 Information Security Audit' which requires individuals completing such assessments and audits to be certified by an international professional or standards association. 'Article 19 Organizations with critical information infrastructure' requires such organizations to introduce standards to ensure information security.
Thailand	The Cyber Security Act B.E. 2562 (2019)[110] includes provisions related to cybersecurity standards and controls. This includes empowering the National Cyber Security Committee to prescribe standards and directions for promoting and developing systems for the provision of services in connection with the cyber security maintenance, establish standards in connection with the cyber security maintenance and prescribe minimum standards relating to computers, computer systems and computer programmes and also promote accreditation of cyber security maintenance standards for critical information infrastructure agencies, State agencies, regulatory or supervisory agencies and private agencies.

[107] https://thedocs.worldbank.org/en/doc/c01714a0bc2ca257bdfe8f3f75a64adc-0070062022/original/Positioning-The-Lao-PDR-for-a-Digital-Future-11-10-22.pdf

[108] Unofficial Translation taken from: https://legalinfo.mn/mn/detail?lawId=16532522791411&showType=1

[109] Unofficial Translation taken from: https://legalinfo.mn/en/edtl/16531350476261

[110] https://cyrilla.org/es/entity/4nywjpircms?page=1

National and Regional Cooperation

The multi-faceted and transnational nature of cybersecurity and cybercrime threats requires countries to foster both internal and external collaborative approaches and mechanisms. This can include domestic based co-operation between government, CNI operators, and the private sector, as well as supporting strong international networks and relationships with foreign law enforcement and national security counterparts.[111]

Southeast Asia Context

The ASEAN Cybersecurity Cooperation Strategy (2021-2025)[112] details that 'regional organisations like ASEAN offer a platform for member states to share and offer regional perspectives, exchange information on emerging and existing threats, implement Confidence Building Measures (CBMs), and build capacity.'

The Strategy contains five dimensions of work:

1. Advancing Cyber Readiness Cooperation;
2. Strengthening Regional Cyber Policy Coordination;
3. Enhancing Trust in Cyberspace;
4. Regional Capacity Building; and
5. International Cooperation.

Interpol[113] is running a multi-year project with the ASEAN which is focused on fostering regional cooperation against cybercrime in Southeast Asia and includes activities such as specialized training courses, table-top exercises, a knowledge base accessible to peers in the region, expert groups in areas of growing concern, and an e-learning course on how to obtain electronic evidence from service providers, including those located in different jurisdictions.

A 2023 report from the International Institute for Strategic Studies[114] acknowledge that ASEAN governments have been bolstering CERT cooperation for more than a decade. The report also outlines regional platforms for cybersecurity cooperation such as the Ministerial Conference on Cybersecurity, the ASEAN Defence Ministers' Meeting Plus Cyber Security Expert Working Group and the ASEAN Regional Forum, and the Inter-Sessional Meeting on the Security of and in the Use of ICT.

Country-Level Activity

Examples of country-level planned, and ongoing national and regional cooperation activity are presented below and provide an indicative insight into the cybersecurity skill requirements to facilitate local and international cybersecurity collaboration.

[111] https://gcscc.ox.ac.uk/cmm-2021-edition

[112] https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

[113] https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/Cyber-Capabilities-Capacity-Development-Project

[114] https://www.iiss.org/research-paper/2023/06/asean-cyber-security-cooperation-towards-a-regional-emergency-response-framework/

Country	Strategic Driver Insights
Cambodia	Cambodia's National Defence Policy 2022[115] includes Cyber Security in Chapter 5 on National Security Protection which includes a range of strategies. Examples include establishing cooperation across national, sub-national, private sector, and NGO stakeholder groups. Cambodia pursues international cooperation activity with such an example including in 2022 with the Japan International Cooperation Agency (JICA) signing a Record of Discussions with the Government of the Kingdom of Cambodia in Phnom Phen for the Project for Improvement of Cyber Resilience, a technical cooperation project.[116]
Indonesia	Indonesia pursues international cooperation activity with such an example including the third Australia-Indonesia Cyber Policy Dialogue held in 2020. This involved a multi-agency Dialogue which covered topics of information sharing, cyber security best practice, capacity building and enhancing digital economy and addressing cybercrime.[117] A 2021 report on Cyber Security Governance in the Indo-Pacific noted that Indonesian Interagency Coordination on cybersecurity is an area that BSSN will seek to lead and improve.[118]
Laos	The 2015 Law on Prevention and Combatting Cyber Crime[119] includes 'Article 7 International Cooperation' which encourages relations and cooperation with foreign countries, and the regional and international community in a campaign of prevention and the combating cybercrime through exchange of lessons, experiences, information, upgrade of technical knowledge and capacity building of technical staffs. Laos pursues international cooperation activity with such an example including participating in The Asia-Pacific Cybercrime (APC) Capacity-Building Hub: an initiative of the Supreme Prosecutors' Office of the Republic of Korea, the World Bank and the Global Forum on Cyber Expertise. This involved Lao PDR joining Cambodia and Papua New Guinea in November 2022 for a training week on national cyber policies, legislation and incident response.[120]
Mongolia	The Mongolia National Cyber Security Strategy[121] includes activity to cooperate with international and regional organizations in the field of cyber security and crime fighting and to seek opportunities to become members of international organizations and join conventions and to ensure the participation of state administrative organizations, the private sector, and non-governmental organizations , and to expand cooperation in ensuring cyber security of small, medium, and start-up business owners, universities, and academic institutions.

[115] https://dot.mod.gov.kh/wp-content/uploads/2022/05/National-Defence-Policy-English.pdf

[116] https://www.jica.go.jp/Resource/english/news/press/2022/20221205_41.html

[117] https://www.internationalcybertech.gov.au/node/1

[118] https://policy-futures.centre.uq.edu.au/files/9577/Policy%20Futures_Cyber%20Security%20Indo%20Pacific_May21.pdf

[119] https://laocert.gov.la/ftp_upload/Cyber_Crime_Law_EnVersion.pdf

[120] https://thegfce.org/the-asia-pacific-cybercrime-apc-capacity-building-hub-an-initiative-of-the-supreme-prosecutors-office-of-the-republic-of-korea-the-world-bank-and-the-global-forum-on-cyber-expertise/

[121] Unofficial Translation taken from: https://legalinfo.mn/mn/detail?lawId=16532522791411&showType=1

	The Law of Mongolia on Cyber Security 2021[122] includes a range of Articles (11.4.4, 14.1.5, 20.3, and 22.2.3) that detail requirements for the domestic and international cooperation of national centres with relevant cybersecurity stakeholders and counterparts. Mongolia pursues international cooperation activity with such an example including a Cyber Security Training Centre to be established in Mongolia with Indian assistance.[123]
Thailand	The National Security Policy and Plan (2019-2022)[124] includes details to develop a framework for international and ASEAN countries cooperation in the prevention and resolution of cyber security problems. The Cyber Security Policy and Action Plan 2022-2027 outlines the vision that "Cybersecurity for Thailand's critical services to ensure economic and social sustainability".[125] Thailand pursues international cooperation activity with such an example including The Ministry of Digital Economy and the National Cyber Security Agency jointly signing a Memorandum of Understanding (MoU) on cybersecurity cooperation with Huawei Technologies.[126] NCSA has also signed separate MoUs on cybersecurity cooperation with the Japan International Cooperation Agency (JICA), the Cyberspace Administration of The People's Republic of China (CAC),[127] and the National Cyber Directorate of the State of Israel (INCD).[128]

Research and Development

Research and development include the exploration of cybersecurity ideas, products, and services to address emerging technological and societal challenges in order to advance the development of cybersecurity knowledge and capabilities that meet national requirements.[129]

Southeast Asia Context

The ASEAN Cybersecurity Cooperation Strategy (2021-2025)[130] does not detail specific cybersecurity research and development activities. It does however acknowledge the need for governments to work with industry, civil society, and academia as part of the development of critical and emerging technologies in order to develop 'innovative solutions that can help make cyberspace safer.'

[122] Unofficial Translation taken from: https://legalinfo.mn/en/edtl/16531350476261

[123] https://president.mn/en/2019/09/21/joint-statement-on-strengthening-the-strategic-partnership-between-india-and-mongolia/#:~:text=JOINT%20STATEMENT%20ON%20STRENGTHENING%20THE%20STRATEGIC%20PARTNERSHIP%20BETWEEN,Modi%2C%20the%20following%20joint%20statement%20has%20been%20issued

[124] https://www.nsc.go.th/wp-content/uploads/2020/05/The-National-Security-Policy-and-Plan2019-%E2%80%932022.pdf

[125] https://www.nstda.or.th/home/knowledge_post/cyber-security-action-plan-2022-2027/

[126] https://www.bangkokpost.com/thailand/pr/2360342/national-cyber-security-agency-signs-mou-with-huawei [119] https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

[127] https://www.bangkokpost.com/life/tech/2340977/des-signs-thai-chinese-mou-on-cybersecurity

[128] https://itrade.gov.il/thailand/event/signing-ceremony-mou-on-cyber-security-cooperation-between-the-state-of-israel-and-the-kingdom-of-thailand/

[129] https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

[130] https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

The ASEAN-Singapore Cybersecurity Centre for Excellence (ASCCE)[131] was established in 2019 and is 'an extension of the ASEAN Cyber Capacity Programme (ACCP) that seeks to conduct research, conduct virtual cyber defence exercises and provide CERT-related technical expertise. It also focuses on other areas such as international law, cyber strategy, legislation, cyber norms among other cybersecurity policy issues.' The Centre has been established to 'deepen the Region's cyber security capabilities and enhance its ability to respond to emerging global cyber threats.'

Country-Level Activity

Examples of country-level planned, and ongoing research and development activity are presented below and provide an indicative insight into the cybersecurity skill requirements to support and secure forthcoming research and innovation.

Country	Strategic Driver Insights
Cambodia	The Cambodia Digital Government Policy 2022-2035[132] includes Strategy 8 Promoting Digital Research and Innovation which acknowledges that digital research and innovation are a key strategy for the increasing capacity, effectiveness, and efficiency of the digital transformation and for ensuring digital competition in the region. Priority actions for this strategy cover areas such as the building of a national system for digital technology research and development, the transfer of digital technology resulting from research to the public and private sectors, and fostering entrepreneurship of digital innovation through the establishment of mechanisms for recognizing fresh innovation and intellectual property protection. Cambodia's National Defence Policy 2022[133] includes Cyber Security in Chapter 5 on National Security Protection which in includes a range of strategies including Research and Development. This acknowledges research and development on cybersecurity as a critical factor to achieve efficient technological advancement and can be achieved through supporting expert teams to research and develop intelligent technology and establish a platform for governmental organizations, NGOs, and private sector to facilitate the exchange of information, knowledge, experience, and technological developments.
Indonesia	The Making Indonesia 4.0 initiative aims to leverage advanced technologies, such as artificial intelligence (AI), the Internet of Things (IoT), advanced robotics, and 3D printing. This will include research and development, as well as design and innovation activities, to improve the ability of the nation in mastering these technologies. Through Making Indonesia 4.0, Indonesia is committed to allocating 2% of GDP to encourage future technology adoption and development.[134]
Laos	A 2022 UNDP Digital Maturity Assessment of Lao PDR[135] found that to support and promote innovation and research, the Government of Lao PDR

[131] https://cybilportal.org/actors/asean-singapore-cybersecurity-centre-for-excellence-ascce/

[132] https://asset.cambodia.gov.kh/mptc/media/Cambodia_Digital_Government_Policy_2022_2035_English.pdf

[133] https://dot.mod.gov.kh/wp-content/uploads/2022/05/National-Defence-Policy-English.pdf

[134] https://www.eria.org/uploads/media/Books/2022-Accelerating-Digital-Transformation-Indonesia/Accelerating-Digital-Transformation-Indonesia-rev3.pdf

[135] https://www.undp.org/laopdr/publications/digital-maturity-assesment-lao-pdr

	enacted the decree on Public-Private Partnership, Law on Intellectual Property, and Law on High Technology.
Mongolia	The Mongolia National Cyber Security Strategy[136] includes activity to support the national production, innovation, research and analysis of information and communication equipment, software, and electronics, and to reduce technological dependence. The Law of Mongolia on Cyber Security 2021[137] includes requirements for government entities to conduct research and analysis on cyber-attacks and violations, and distribute recommendations and information thereon to the public (22.2.2) and to conduct new technical, technological, innovation, research and development activities in areas of cyber security (12.1.7).
Thailand	The Cyber Security Act B.E. 2562 (2019)[138] empowers the National Cyber Security Committee to study and research into information necessary for the cyber security maintenance with a view to making recommendations on cyber security maintenance measures and provide regular training and practice on cyber threat handling to agencies concerned. In addition, the act sets out policy and plan goals on cyber security maintenance in Thailand which includes Section 42(5) the research and development of technology and bodies of knowledge relating to the cyber security maintenance.

Conclusion

This chapter identified nine cybersecurity strategic drivers for skills for the five research focus countries. Indicative examples of activity for each strategic driver have been provided for each country to establish an understanding of the goals and forces that are driving the need for technical cybersecurity skills to ensure that such activities and capabilities can be developed and deployed securely.

The information presented in this strategic drivers chapter will be analysed in the Future Workforce Assessment in order to determine what technical cybersecurity functions, teams, roles, and competencies will be required.

[136] Unofficial Translation taken from: https://legalinfo.mn/mn/detail?lawId=16532522791411&showType=1

[137] Unofficial Translation taken from: https://legalinfo.mn/en/edtl/16531350476261

[138] https://cyrilla.org/es/entity/4nywjpircms?page=1

Chapter 2: Participation of Women in the Cybersecurity Workforce

Introduction

This chapter presents insights on the current cybersecurity workforce context and the participation of women in the cybersecurity workforce in the Southeast Asian region and explores topics including understanding the current situation and initiatives, identifying barriers that need to be addressed to improve female participation rates, and the different opportunities that could be explored to close the gap.

The insights from this chapter will be combined with the findings from future steps in the research project to inform recommendations to ensure women in cybersecurity play an active part in the achievement of a prosperous and secure future across the Southeast Asian region.

Methodology

Data Collection

This chapter was informed by a series of one-on-one interviews completed with seven participants with knowledge of women's participation in the cybersecurity workforce environment in the Southeast Asian region. A semi-structured interview approach was utilised, and the interview guide is detailed in Annex B.

Insights captured during the interviews have been supplemented by some additional evidence drawn from sources identified using desk-based research which are included in the footnotes.

Research Participants

Representatives from each of the five research focus countries that are working in or with knowledge of the cybersecurity workforce environment were invited to participate in the one-on-one interviews. These included a combination of stakeholders including:

- Academia
- Civil Society Organisations
- Cybersecurity Training Organisations
- International Development Organisations
- Private Sector

Details of the interview participant profile are provided in Annex B.

Research Limitations

This research relied on a combination of purposive and snowball sampling of interview participants. The findings in this chapter are not presented as a representative sample or complete analysis of the participation of women in the cybersecurity workforce environment across the Southeast Asian region.

Participants from government organisations were not available for interviews during the research period and as such the insights in this chapter represent a non-government stakeholder viewpoint on the topic.

This research was not intended to be and should not be taken as a comprehensive assessment, rather it provides an indicative representation of the key themes that will be utilised to design general recommendations for the developing the cybersecurity workforce and participation of women in the Southeast Asian region.

General cybersecurity workforce situation

This section details insights captured from the interviews on the general state of the cybersecurity workforce in the research focus countries.

National Workforce Context

- **Workforce and Skills Shortages:** Interview participants acknowledged that, consistent with other regions of the world, there was a shortage of both cybersecurity workers as well as cybersecurity skills across the workforce and broader society.

    - Examples of evidence of this shortage shared by participants included the absence of cybersecurity role job postings on popular employment websites as well as cybersecurity related government departments having problems filling a large number of current vacancies.
    - An example shared of an exception to this cybersecurity workforce and skills shortage included that certain critical infrastructure organisations such as financial institutions were much more likely to have cybersecurity professionals in place.

- **Transitioning Workforce:** It was acknowledged that countries in the region are at different stages of digital transformation and economic development. As such the need for a technical workforce is only emerging in some countries and is expected to accelerate in coming years.

- **IT Roles:** It was noted that cybersecurity functions often fall on the shoulders of IT departments and managers and is not typically identified as a separate function.

> *"It's improving but the workforce has only really started to develop into a non-agrarian workforce. There's not a very developed cybersecurity workforce here or technical workforce at all."*

- **Digital Transformation Impact:** Participants were not aware of specific cybersecurity workforce development priorities in their countries but there was a consistent view that digital transformation and cybersecurity was an increasing focus for governments in the region. Such increased attention was also evident from the international development community, with funding for cybersecurity training often forming part of larger digital upskilling programs.

- **Lower Priority:** Several participants agreed that cybersecurity in general had not necessarily been a priority in their country in the past which has seen limited investment and attention in filling related workforce and skills gaps.

Challenges for Workforce Development

Interview participants identified a wide range of challenges in their countries when it comes to national cybersecurity workforce development including:

- **Low Awareness:** A general lack of awareness of the cybersecurity risks to both individuals and organisations which therefore limits the ability to identify the skills and capabilities required to respond to such cybersecurity threats.

    - Low levels of awareness amongst students and the general population on cybersecurity as a career pathway.
    - Lack of knowledge and support for primary and secondary school teachers on cybersecurity as a career pathway for their students.
    - Lack of awareness of the prospects and benefits of cybersecurity careers amongst parents which typically have a strong influence over their child's study pathways.
    - Misconceptions across the population that cybersecurity is a technical field for specialists only.

- **Cybersecurity Culture:** A culture that cybersecurity is not an individual's problem with an expectation amongst internet users that it is the government's role to shoulder responsibility for cybersecurity and individuals do not see it as their own responsibility.

- **Limited Curriculum:** Limited cybersecurity related content as part of primary and secondary school curriculum.

- **Minimal Outreach:** Lack of investment in cybersecurity career outreach programs from government and education stakeholders such as universities.

- **Accessibility and Availability:** Barriers related to cybersecurity training pathways including accessibility and costs barriers, limited training provider options and formal learning pathways outside of university courses, which in themselves were not commonly available.

- **Coordination:** Coordination challenges across government and lack of clarity of which agencies are empowered and responsible to advance cybersecurity workforce development initiatives.

> *"People don't really understand the importance of cybersecurity or digital security in their work or their life. So that's why they don't, you know, study this course, or try to find all of this information to be one of the experts."*

Current Initiatives

Interview participants outlined some examples of current initiatives in their countries to encourage the development of a cybersecurity workforce including:

- **Community Building:** Creating a community of cybersecurity professionals for networking and development.

- **Awareness:** Ad-hoc awareness initiatives such as cybersecurity career talks at youth camps by current cybersecurity professionals and academics.

- **Partnerships:** Public-Private partnerships between government and technology companies to support the inclusion of cybersecurity in schools and university curriculum.

- **Government Courses:** Government agencies running digital security courses that are available to the public.

- **In-House Training:** Private sector initiatives to offer in-house cybersecurity training to upskill staff.

Insights from Existing Research

Further to the insights captured in the interviews, some key insights related to the cybersecurity workforce situation in Southeast Asia include:

- A 2022 (ISC)[2] Cybersecurity Workforce Study estimated the existing global cybersecurity workforce at 4.7 million, with a worldwide gap of 3.4 million cybersecurity workers. Of those, approximately 860 thousand were based in the Asia-Pacific, which registered the highest year on year from of 15.6%.[139]

- A 2022 report[140] from the Asian Development Bank on Digital Jobs and Digital skills in Asia and the Pacific including some key findings such as:

    - Demand for digital skills has steadily increased over the past 5 years.
    - Demand for digital skills grew most in industries hit hardest by the pandemic.
    - Basic digital literacy is now essential, and workers with higher skills benefit more.
    - Short- and medium-duration online digital skill training programs witnessed high growth rates in the past year.
    - Equal access to digital skills and credentials by gender requires affirmative action.

[139] https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx
[140] https://www.adb.org/sites/default/files/publication/829711/digital-jobs-digital-skills.pdf

Participation of Women in the Cybersecurity Workforce

This section details insights captured from the interviews on the participation of women in the cybersecurity workforce in the research focus countries.

Current participation levels

- **Low Participation:** Interview participants all indicated that the current level of participation of women in cybersecurity careers in their countries low with anecdotal estimates ranging from five percent up to 25 percent.

- **Gradual Improvement:** Participants did note that whilst this base level of participation is low there have been gradual improvements and clear positive trajectory in the number of women both enrolling in cybersecurity training courses as well as entering the workforce in cybersecurity roles. Despite this increase in training enrolments, several participants noted that they were unsure and had concerns about the level of attrition before reaching the workforce.

- **Limited Senior Roles:** Whilst it was acknowledged by participants that there were some positive signs in the participation of women in the cybersecurity workforce, such participation was typically concentrated in more junior roles and that participation rates at senior management level were still very low.

> *"It does seem to be more male dominated, but I do see women in some of those roles like in IT help desk roles which typically also cover cybersecurity at a basic level. So, there are more and more women in the workforce, but it tends to be as we said more male dominated"*

> *"It is still a huge gender gap in terms of engagement from women in the cyberspace."*

Perceived benefits

Interview participants shared their views on the benefits they expect to see from increasing the participation of women in the cybersecurity workforce including at a societal level as well as for women working in cybersecurity careers.

Benefits to countries/society

Participants noted that increasing the participation of women in the cybersecurity workforce would provide a range of benefits across all levels of society including:

- **Improved Solutions:** Developing more effective cybersecurity solutions for end users by improving the understanding of women and girls' digital experiences, preferences, and behaviours.

- **Diverse Workforce:** The positive impact that a more diverse workforce can have for the efficiency and effectiveness of cybersecurity teams and improving the combination of soft skills and technical skills. Several participants indicated that soft skills such as communication, detail-orientation, problem-solving, and empathy are typically more common workforce traits for women in their country.

- **Threat Mitigation:** Increasing the diversity of ideas to help predict and prevent cyber threats.

- **Inspire Future Generation:** Increasing the reach of cybersecurity and cyber safety programs with women in cybersecurity roles helping to inspire girls and other women to take their digital security and safety seriously as well as building their aspiration and confidence to pursue cybersecurity training and career pathways. This in turn will also support women to more fully participate in the digital economy and drive economic growth.

- **Break Stigmas:** Helping to break stigmas around women's capabilities and role in society and challenges perceptions that only a man can complete more technical and specialist roles in the workforce.

- **Increase Resource Base:** Providing a larger resource base to draw from to help countries address cybersecurity workforce and skills gaps and support the full utilization of the labour market and the economic benefits that this would bring.

> *"At the end of the day, we've got a huge gap. You've got 50% of the population. They're able, they're capable, you can help fill that gap."*

> "If women actually understand cyber security and how important this issue is for them, it actually will decrease the number of online gender-based violence… to understand how important their digital safety is and how aligned this issue actually is with their safety online."

Benefits to Women in Cybersecurity

Participants noted that increasing the participation of women in the cybersecurity workforce would also provide benefits to the women pursuing such careers including:

- **Salary:** Securing roles in a profession that has higher than average salaries.

- **Familial Stability:** Cybersecurity is seen as a career with strong long-term prospects that can drive economic development for women and increase familial stability.

> *"You can have like good life, and a good salary, a good future. You can help protect your friends, your family, even protect your nation."*

Barriers and challenges

Interview participants identified a wide range of challenges in their countries when it comes to the participation of women in the cybersecurity workforce including:

- **Societal Expectations:** Societal expectations of women's role in family and pressure to leave the workforce if they get married, have children, need to look after a parent, all of which then impacts hiring choices for employers. Also, in some cases when families have limited resources and multiple children, they might prioritise sending a son to university instead of their daughter as they expect this will provide a greater economic benefit to the family.

- **Gender Perceptions:** Perceptions that boys are generally better with computers, discouraging girls to participate in related activities during schooling and ingraining notions that more technical study areas are too hard for woman.

- **Discrimination:** Women are currently the minority in cybersecurity training classes and face discrimination and isolation during their study.

- **Cost:** There is often a high cost to complete cybersecurity training courses or university study and women often rely on scholarships to pursue such education pathways.

- **Access to Promotions:** Even when women make it into cybersecurity roles that have trouble gaining promotions to senior and leadership roles due to stereotypes that men are better suited for such positions.

- **Low Visibility:** With less women in the cybersecurity workforce there is less visibility for aspiring professionals to see role models that they can aspire to and talk with to gain confidence and build aspiration to pursue their own cybersecurity career.

- **Hiring Practices:** Instances where job advertisements for cybersecurity roles specific that they are looking for male candidates.

> *"There are barriers I think both from kind of the access side, the awareness raising side and the ability to have mentorship and peer networking that can help build sustained engagement in the space."*

> *"They have to overcome a lot of like humiliation, feeling alone, being there…and proving constantly, 'I can do that', is something like not everyone can survive."*

Participation and retention activities

Interview participants identified examples of activities they are aware of to encourage the participation and retention of women in the cybersecurity workforce including:

- **Coding Clubs:** Female coding clubs to help open doors for girls to technology relate fields.

- **After School Programs:** After school programs for girls in middle and high school to provide beginner level knowledge on topics such as website building and online security.

- **Upskilling Staff:** Private sector and civil society organisations funding training and development of female staff to upskill in cybersecurity subject areas.

- **Digital Skill Development:** Digital upskilling programs for women to use tech as a tool for career-building.

- **Networking:** Networking sessions for women in tech that involve casual meet-ups with talks and panel discussions and connect aspiring young professionals with experts.

- **Meaningful Work:** Anecdotal evidence of government agencies making efforts to given women in the cybersecurity workforce more important and meaningful tasks as part of their roles.

> *"Look I sometimes, I'm just having a feeling that the retention of women in the workforce and gender equality is being remembered during the 8th of March, the Women's International Day. Being a woman myself and I kind of like, what, you're thinking about that one day a year. This is when the most discussions happen both in [business and in the] media, but otherwise like I have not at least been a witness of any intervention long term."*

Ideas and recommendations for future interventions

Lastly, interview participants shared their ideas and recommendations for future interventions to increase the participation of women in the cybersecurity workforce including:

- **Terminology:** Reflecting on the impact of the language used to discuss this topic and how women should not just be participating in but also leading the cybersecurity workforce.

- **Articulating Benefits:** Improving the messaging around the potential benefits of increasing the number of women in the cybersecurity workforce not just in terms of providing opportunities for employment and fulfilling careers but also the broader economic, social, and security impacts that this brings through the full utilisation of the labour market. As part of such activity consider a range of both traditional, as well as more modern communication channels such social media influences to reach target audiences.
- **Partnerships:** Collaboration between public, private, and civils society stakeholders to raise awareness of the diverse range of cybersecurity careers and training pathways.

- **Success Stories:** Sharing success stories of women in cybersecurity leadership roles.

- **Visibility and Mentoring:** Increasing the visibility of female role models working in cybersecurity and other technical fields to aspiring professionals and develop networking, mentoring, and internships programs to bring them together.

- **Business Owners and Entrepreneurs:** Consider initiatives that also focus on equipping female business owners and entrepreneurs in cybersecurity skills required to ensure they realise and protect the full benefits of that can be gain from the emerging digital economies.

- **Regulation and Accreditation:** Consider the role of regulation and accreditation to better formalise cybersecurity training pathways and make it easier for women to understand and pursue learning pathways that lead to cybersecurity roles.

- **Affirmative Action and Incentives:** Explore policies and initiatives around affirmative action and women in cyber scholarships to incentivise and accelerate interest and growth in cybersecurity training and workforce development for women.

- **Enabling Work Environment:** Create enabling and flexible work environments that align with the diverse sociocultural context of women in the Southeast Asian region such the ability to work from home.

- **Cohort Approach:** Consider developing programs that identifies and supports a cohort of women to go through a holistic program that combines these ideas of awareness raising, cyber capacity building, skills and workforce development, peer networking, and mentoring.

- **School Level Initiatives:** Increase the range of initiatives targeted at girls during primary and secondary school to promote cybersecurity such as curriculum, competitions, and other initiatives with a youth focus.

> *"You have to make young people believe in themselves, give them trust and confidence, and give them the opportunity to work with the successful [female cybersecurity professionals] to inspire them. I think this is the way to gain more women in this area of work."*

> *"Creating a holistic programme where you get a lot of ministries and a lot of investment focused on a cohort of women, say it's 200, say it's 300 within a particular country, I think that would be so successful and such a great use of money spent."*

Insights from Existing Research

Further to the insights captured in the interviews, some key insights related to the participation of women in the cybersecurity workforce in Southeast Asia include:

- A 2018 (ISC)[2] Cybersecurity Workforce Report on Women in Cybersecurity[141] found that women accounted for 24% of the overall global cybersecurity workforce.

- A 2021 report[142] from The Asia Foundation on accelerating women's advancement in STEM found that "Networks, both formal and informal, play a pivotal role in helping girls and women enter and succeed in STEM fields. They do this by facilitating peer support, role models, mentorship and sponsorship, opportunities for technical and soft skills development, knowledge exchange and collaboration, visibility, and more."

- A 2020 Action Brief[143] from UN Women on Women, Peace, and (Cyber) Security in Asia and the Pacific found that "there is a significant gender gap in cybersecurity - in Asia and the Pacific, women account for less than 10% of the cybersecurity workforce. This gap in women's participation has resulted in a lack of gender perspectives informing cybersecurity and the development of cybersecurity frameworks that fail to identify and respond to cyberthreats faced by women and girls." The Action Brief notes that "Increasing women's participation in cybersecurity and decision-making relating to the digital world is a crucial step to ensuring that the spectrum of cyber risks is addressed. Women are best placed to identify their unique cybersecurity needs and contribute their lived experiences to the knowledge-base, informing cybersecurity, yet their representation remains low."

---

[141] https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx?la=en&hash=4C3B33AABFBEAFDDA211856CB274EBDDF9DBEB38

[142] https://asiafoundation.org/wp-content/uploads/2021/06/Accelerating-Womens-Advancement-in-STEM_Report.pdf

[143] https://asiapacific.unwomen.org/sites/default/files/Field%20Office%20ESEAsia/Docs/Publications/2020/06/Action%20Brief%20%20WPS%20%20CYBERSECURITY16620final.pdf

Conclusion

This chapter detailed insights into the participation of women in the cybersecurity workforce in the Southeast Asia region. This included details on the current cybersecurity workforce situation and the various initiatives being implemented to close workforce gaps as well as various barriers that need to be addressed and opportunities to explore in improving the participation rate of women in the cybersecurity workforce.

The information presented in this chapter will help to inform the analysis approach to the Future Workforce, Market, and Gap Assessments and to identify opportunities to increase the participation of women in the cybersecurity workforce across the Southeast Asian region.

Chapter 3: Future Workforce Assessment

Introduction

This chapter presents a high-level assessment of the future workforce requirements of the five research focus countries based on the nine strategic drivers identified and defined in the Strategic Drivers chapter. This future workforce assessment extrapolates the technical cybersecurity roles and additional skills that will be required as a priority for the five research focus countries to facilitate the realisation of cybersecurity capacity building targets in response to each strategic driver.

The technical cybersecurity roles and additional skills identified in this chapter provide insight into the expected demand side of the cybersecurity workforce ecosystem and combined with the market assessment will be used to inform the gap assessment.

Methodology

Assessment Approach

The Future Workforce Assessment extrapolates priority technical cybersecurity roles and additional skills required based on the nine strategic drivers previously defined in the Strategic Drivers chapter:

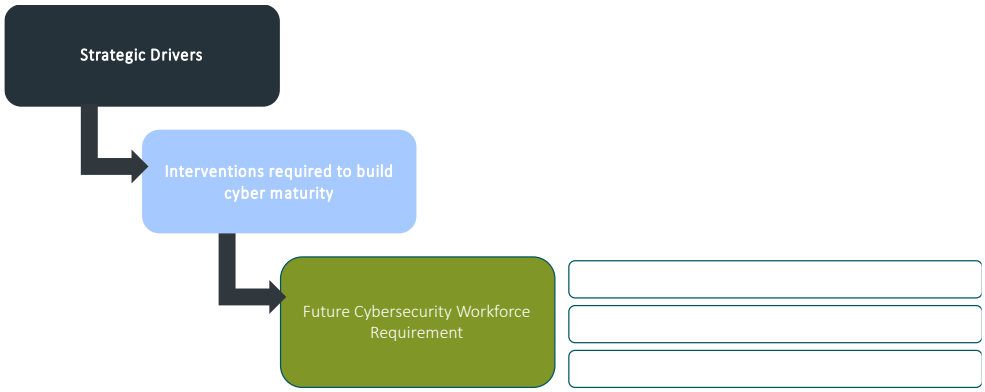
1. Principal National Cybersecurity Risks
2. Digital Transformation
3. Legislation and Regulation
4. Critical National Infrastructure
5. National Security and Criminal Justice System
6. Incident Response
7. Security Standards and Controls
8. National and Regional Cooperation
9. Research and Development

For each strategic driver, extrapolation of technical cybersecurity roles and additional skills includes the following process:

- identifying interventions that will be required to build national cybersecurity capacity maturity in response to each strategic driver.
- determining the cybersecurity workforce teams/functions that will be necessary to implement such interventions.
- identifying the required priority technical cybersecurity job roles for such teams/functions to implement such interventions.
- identifying any additional cybersecurity skills required for the non-specialist workforce.

This process is illustrated in Figure 1.

Figure 1 - Future Workforce Assessment Process



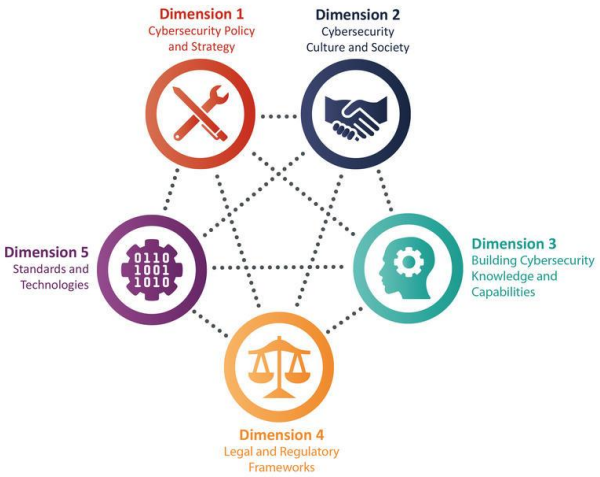
National cybersecurity capacity maturity

To assist with identifying interventions that will likely be required to increase cybersecurity capacity maturity in response to the nine strategic drivers, the Oxford Cybersecurity Capacity Maturity Model for Nations (CMM)[144] is utilised to guide what capacity and capability will need to look like at these higher levels of maturity. The CMM *"helps nations understand what works, what does not work and why, across all areas of cybersecurity capacity. This is important so that governments and enterprises can adopt policies and make investments that have the potential to significantly enhance safety and security in cyberspace, while also respecting human rights, such as privacy and freedom of expression."*

Dimensions of National Cybersecurity Capacity

The CMM considers national cybersecurity capacity to comprise five Dimensions which together constitute the breadth of national capacity that a country requires to be effective in delivering cybersecurity:[145]

Figure 2 - CMM Dimensions



[144] https://gcscc.ox.ac.uk/cmm-2021-edition
[145] https://gcscc.ox.ac.uk/the-cmm

Cybersecurity Workforce and Skills Frameworks

There are several established national and regional cybersecurity workforce and skills frameworks that provide valuable guidance on the range of cybersecurity knowledge areas, team functions, job roles and competencies required to establish a robust and resilient cybersecurity capability and workforce. Examples of such leading frameworks include:

Australian Signals Directorate Cyber Skills Framework[146]

"The ASD Cyber Skills Framework defines the roles, capabilities and skills proficiencies that are essential to cyber missions, and that can be used in both the security and offensive contexts. The ASD Cyber Skills Framework is relevant to wider government, industry and academia which can be implemented and used as a tool for understanding and profiling cyber skills in any organisation."

Canadian Cyber Security Skills Framework[147]:

"The Canadian Cyber Security Skills Framework is based on elements of the U.S. NICE Workforce Framework for Cybersecurity (NICE framework), contextualized for the Canadian labour market. It's a model that leverages the NICE framework while simplifying it using a business-oriented lens recognizing talent from an organizational security perspective and is a model more accessible to non-cyber security stakeholders."

European Cybersecurity Skills Framework (ECSF)[148]:

"The European Cybersecurity Skills Framework (ECSF) is a practical tool to support the identification and articulation of tasks, competences, skills and knowledge associated with the roles of European cybersecurity professionals. It is the EU reference point for defining and assessing relevant skills, as defined in the Cybersecurity Skills Academy, which was recently announced by the European Commission."

Saudi Cybersecurity Workforce Framework (SCyWF)[149]:

"The SCyWF categorizes cybersecurity work in Saudi Arabia, defines the job roles within each category and sets the requirements for each job role in terms of tasks, knowledge, skills and abilities (TKSAs). The main objective of the SCyWF is to serve as a reference model and a guideline for preparing, developing, recruiting, promoting and managing the cybersecurity workforce. It provides a common lexicon that improves communication and content development for talent management activities. It also helps in mapping learning outcomes of education and training programs to the knowledge, skills and abilities (KSAs) required for different cybersecurity job roles."

Singapore Skills Framework for Infocomm Technology (ICT)[150]:

"The Skills Framework for ICT is a guide for individuals, employers, and training providers to promote ICT skills mastery and lifelong learning. It can be used by employers to develop career maps and articulate job requirements, used by individuals to guide their skills identification and development to stay relevant, and used by training providers to devise ICT courses. Some critical skill areas include

[146] https://www.asd.gov.au/sites/default/files/2022-10/ASD-Cyber-Skills-Framework-v2.pdf
[147] https://www.cyber.gc.ca/sites/default/files/canadian-cyber-security-skills-framework-may-2023-v2.pdf
[148] https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework
[149] https://nca.gov.sa/files/scywf_en.pdf
[150] https://www.imda.gov.sg/how-we-can-help/techskills-accelerator-tesa/skills-framework-for-infocomm-technology-sfw-for-ict

network and infrastructure, software development and engineering, data and analytics, and cyber-security."

UK Cyber Security Council Cyber Career Framework[151]:

"This section provides details about the 16 specialisms in cyber security and suggests pathways through and between them. It's a flexible definition that individual practitioners - current or future - can use to plan out a possible career; it's not a standard to be followed rigidly…Details include an introduction to each specialism, information on the typical responsibilities and tasks, the skills and knowledge required, and information on useful prior experience for those hoping to enter the specialism from outside cyber security. Information also includes a list of common job titles and average salary ranges."

US Workforce Framework for Cybersecurity (NICE Framework)[152]:

"The NICE Framework provides a set of building blocks for describing the tasks, knowledge, and skills that are needed to perform cybersecurity work performed by individuals and teams. Through these building blocks, the NICE Framework enables organizations to develop their workforces to perform cybersecurity work, and it helps learners to explore cybersecurity work and to engage in appropriate learning activities to develop their knowledge and skills."

Framework to inform Future Workforce Assessment

For the purpose of this Future Workforce Assessment, the 'European Cybersecurity Skills Framework' has been selected to classify the technical cybersecurity job role requirements. This was chosen as it is a regional model with applications to multiple member countries providing parallels to the Southeast Asian region and could inform an approach for an ASEAN equivalent regional cybersecurity skills framework. Further details on the 'European Cybersecurity Skills Framework' are provided in Annex C.

[151] https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/
[152] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

Southeast Asia Cybersecurity Future Workforce Assessment

An analysis table is detailed in Annex B which provides a high-level view of how the nine strategic drivers link to future cybersecurity capacity maturity and the associated priority technical cybersecurity job roles required to support such activity. A breakdown summary of the future workforce requirement from this analysis is provided below.

Cybersecurity Workforce Functions and Teams

For the five research focus countries to reach their digital transformation and cybersecurity capacity development ambitions, a range of cybersecurity workforce functions and teams are required to facilitate and secure such activity. Based on the analysis of the strategic drivers in Annex C, the following key workforce functions and teams have been identified to fulfil such requirements:

Table 1 - Required Functions/Teams for each Strategic Driver

Strategic Driver	Required Functions/Teams

1. Principal National Cybersecurity Risks	• National Security Function
	• National Cybersecurity Function / National Cyber Security Centre
	• National CERTs / Incident Response Function
	• Teams responsible for Cybersecurity/SOC within:
	  ○ Public Sector Ministries/Departments
	  ○ Private Sector Organisations
	  ○ Civil Society Organisations

2. Digital Transformation	• eGovernment Providers • eCommerce Providers • ISPs • Internet Infrastructure Operators • Government Digital Transformation Agency

3. Legislation and Regulation	• National Cybersecurity Legislation and Regulation Compliance Function
	• National Telecommunications Regulator
	• Sector Specific Regulators where they exist.
	• National Data Protection Agency
	• CNI Assets/Operators
	• Teams responsible for Cybersecurity Legislative and Regulatory compliance within:
	  ○ Public Sector Ministries/Departments
	  ○ Private Sector Organisations
	  ○ Civil Society Organisations

4. Critical National Infrastructure	• CNI Assets/Operators • National Cybersecurity Function / National Cyber Security Centre • CNI Monitoring and Compliance Function • National CERTs / Incident Response Function • Sectoral CERTs / Incident Response Function
5. National Security and Criminal Justice System	• National Security Function • Defence Force • Police Force • Prosecutors • Courts and Judges
6. Incident Response	• National CERTs / Incident Response Function • Sectoral CERTs / Incident Response Function • CNI Assets/Operators

	• National Cybersecurity Function / National Cyber Security Centre
	• ISPs
	• Teams responsible for Cybersecurity/SOC within:
	  ○ Public Sector Ministries/Departments
	  ○ Private Sector Organisations
	  ○ Civil Society

7. Security Standards and Controls	• National CERTs / Incident Response Function
	• Sectoral CERTs / Incident Response Function
	• CNI Assets/Operators
	• National Standards Agency
	• Cybersecurity Standards and Controls Compliance Function
	• ISPs
	• Teams responsible for Cybersecurity/SOC within:
	  ○ Public Sector Ministries/Departments
	  ○ Private Sector Organisations
	  ○ Civil Society Organisations

8. National and Regional Cooperation	• Transitional Crime Teams
	• National Security Function
	• Defence Force
	• National CERTs / Incident Response Function
	• Sectoral CERTs / Incident Response Function
	• Teams responsible for Cybersecurity/SOC within:
	  ○ Public Sector Ministries/Departments
	  ○ Private Sector Organisations
	  ○ Civil Society Organisations

9. Research and Development	• Government Ministry for ICT/Cybersecurity
	• National Cybersecurity Function / National Cyber Security Centre
	• National Telecommunications Regulator
	• Research and Innovation Functions
	  ○ Public Sector
	  ○ Private Sector
	  ○ Civil Society Organisations

Priority Technical Cybersecurity Roles

The organisations within which these functions/teams sit, or will sit, may currently have some specialist cyber security staff in defined job roles or alternatively they may currently have some staff with the knowledge, skills and ability to fill some of these roles. Either way, given the required growth in the number, scale and scope of these functions/teams implied by the strategic drivers, every organisation is likely to have to create or scale up the capacity and capability over the next five years.

This scaling up of capacity will require additional staff in each identified job role, with an initial focus on entry and practitioner level staff and then overtime building up to more senior practitioners and team leaders.

Based on the analysis of the strategic drivers in Annex C, Table 2 details the Technical Cybersecurity Job Roles that have been identified as priorities for the five research focus countries.

Table 2 - Priority Technical Cybersecurity Jobs Roles for each Strategic Driver

Strategic Driver	Priority Technical Cybersecurity Job Roles
1. Principal National Cybersecurity Risks	• Chief Information Security Officer (CISO) • Cyber Incident Responder • Cyber Threat Intelligence Specialist • Cybersecurity Educator • Penetration Tester
2. Digital Transformation	• Chief Information Security Officer (CISO) • Cyber Incident Responder • Cyber Legal, Policy & Compliance Officer • Cyber Threat Intelligence Specialist • Cybersecurity Architect • Cybersecurity Auditor • Cybersecurity Educator • Cybersecurity Implementer • Cybersecurity Risk Manager • Penetration Tester
3. Legislation and Regulation	• Cyber Legal, Policy & Compliance Officer • Cybersecurity Auditor • Cybersecurity Risk Manager
4. Critical National Infrastructure	• Chief Information Security Officer (CISO) • Cyber Incident Responder (including ICS/OT capabilities) • Cyber Legal, Policy & Compliance Officer • Cyber Threat Intelligence Specialist • Cybersecurity Architect • Cybersecurity Auditor • Cybersecurity Implementer • Cybersecurity Risk Manager • Digital Forensics Investigator • Penetration Tester
5. National Security and Criminal Justice System	• Cyber Threat Intelligence Specialist • Cybersecurity Educator • Digital Forensics Investigator • Penetration Tester
6. Incident Response	• Cyber Incident Responder

	• Cyber Threat Intelligence Specialist • Digital Forensics Investigator • Penetration Tester
7. Security Standards and Controls	• Chief Information Security Officer (CISO) • Cyber Legal, Policy & Compliance Officer • Cybersecurity Architect • Cybersecurity Auditor • Cybersecurity Implementer • Cybersecurity Risk Manager
8. National and Regional Cooperation	• Cyber Incident Responder • Cyber Threat Intelligence Specialist • Digital Forensics Investigator • Penetration Tester
9. Research and Development	• Chief Information Security Officer (CISO) • Cyber Threat Intelligence Specialist • Cybersecurity Implementer • Cybersecurity Researcher

Figure 3 provides a visual mapping of these Priority Technical Cybersecurity Jobs Roles for each Strategic Driver.

This mapping provides a national level view of Priority Technical Cybersecurity Job Roles and individual organisations are encouraged to complete their own targeted workforce needs analysis to identify the specific technical cybersecurity roles necessary for them to successfully perform their respective mission and deliver on their objectives. Such targeted workforce needs analysis will also allow organisations to identifying the volume and proficiency level requirements for each role.

Figure 3 - Mapping of Priority Technical Cybersecurity Job Roles by Strategic Drivers

European Cybersecurity Skills Framework Role Profiles	Strategic Drivers								
	Principal National Cybersecurity Risks	Digital Transformation	Legislation and Regulation	Critical National Infrastructure	National Security and Criminal Justice System	Incident Response	Security Standards and Controls	National and Regional Cooperation	Research and Development
Chief Information Security Officer (CISO)	■	■		■			■		■
Cyber Incident Responder	■	■		■		■		■	
Cyber Legal, Policy and Compliance Officer		■	■	■			■		
Cyber Threat Intelligence Specialist	■	■		■	■	■		■	■
Cybersecurity Architect		■		■			■		
Cybersecurity Auditor		■	■	■			■		
Cybersecurity Educator	■	■			■				
Cybersecurity Implementer		■		■			■		■
Cybersecurity Researcher									■
Cybersecurity Risk Manager		■	■	■			■		
Digital Forensics Investigator				■	■	■		■	
Penetration Tester	■	■		■		■		■	

Recommended Starting Point for Key Technical Cybersecurity Roles

The analysis above details the need for the development of a cybersecurity workforce that includes all 12 role profiles presented in the European Cybersecurity Skills Framework. Whilst it is crucial that countries consider the need for all of these roles as part of their workforce activity, we recommend selecting a few roles as a starting point to focus on and then build on these overtime. As such the following five roles have been identified for consideration as key candidate technical cybersecurity roles for the five research focus countries:

1. Cyber Incident Responder
2. Cyber Legal, Policy, and Compliance Officer
3. Cyber Threat Intelligence Specialist
4. Cybersecurity Risk Manager
5. Penetration Tester

These roles have been selected as they will be required in response to several of the Strategic Drivers as well as having responsibilities for core functions of an organisation's cybersecurity operation. In addition, consideration should be given to having senior representation of these five roles, that may come from within the five listed, or be an addition to them. It could be a CISO, as described by the 12 role profiles, or other managerial or leadership role such as the Head of IT who would be expected to have a good level of understanding of technical cybersecurity.

Additional Cybersecurity Workforce Requirements

In addition to the priority technical cybersecurity roles identified, in order for organisations to build resilience to the increasing cybersecurity risks and threat environment, it is important that organisations develop cybersecurity awareness and capabilities across the whole workforce. These additional requirements are summarised in Table 3.

Table 3 - Additional Cybersecurity Workforce Requirements for Each Staff Category

Staff Category	Additional Requirements	Knowledge and Skills
Senior Executives	Senior staff need to be able to develop and embed cybersecurity strategies and policies as part of the organisations culture.	Develop organisational cybersecurity strategies and culture.
Managers	Managers should develop a basic understanding of cybersecurity principles and how to apply organisational policies across their teams.	Understand security principles and apply security policies.
IT Staff	IT Staff require basic response and investigation techniques.	Knowledge of: • Information security management principles of Hacker techniques • Incident response and investigation • Network security
General Workforce	All staff have a general understanding of how to keep themselves, organisational assets and their families safe in cyberspace.	The general workforce is likely to require knowledge of networking security and information security management principles, and be able to recognise and appropriately respond to common threats that seek to exploit system, network and human vulnerabilities.

Participation of Women in the Future Cybersecurity Workforce

This chapter has identified the priority technical cybersecurity job roles that will be required in response to nine strategic drivers. Each role has been defined utilising the European Cybersecurity Skills Framework (ECSF) which provides a range of details through a role profile role that covers key attributes including:

- Role Title
- Alternative Titles
- Summary Statement
- Mission
- Deliverables
- Tasks
- Knowledge
- Skills
- Competencies

This combination of priority role identification and role profile attributes can be utilised to inform both general workforce development policies and activities as well as interventions specifically

targeted at increasing the participation in the cybersecurity workforce such as raising awareness of specific cybersecurity roles, building aspiration for a range of cybersecurity career pathways, clearly defining job role requirements, and mapping education and training pathways that will equip prospective cybersecurity professionals with the knowledge, skills, and abilities to pursue a successful cybersecurity career.

In addition, this future workforce assessment identified a wide range of cybersecurity functions and teams that will be required for the five research focus countries to reach their digital transformation and cybersecurity capacity development ambitions. A key component of each country's response to building up the scale of their cybersecurity workforce in response to these requirements will be ensuring the full utilisation of the labour market, with the participation of women and any other underrepresented groups playing a key role in achieving this full utilisation objective.

Conclusion

The future workforce needs identified in this chapter provide an understanding of the technical cybersecurity workforce job roles and associated skills required across all involved organisations for the five research focus countries to fulfil their digital transformation and cybersecurity capacity development ambitions and respond to and mitigate the risk from the growing cyber threat landscape.

Through establishing these demand-side elements of the cybersecurity workforce ecosystem, it is now possible to determine the education and training supply-side elements that will be required to service such demand. This will be completed via a market assessment of existing education and training provision that will then be combined with the future workforce assessment to inform a gap assessment to understand focus areas that need to be addressed in order to reduce cybersecurity workforce supply and demand disparities.

Chapter 4: Market Assessment

Introduction

This chapter presents a market assessment of the current cybersecurity skills base in each of the five research focus countries organised into four categories of (i) Primary and Secondary School, (ii) Higher Education and Research, (iii) Professional Training and Certification, and (iv) Public and Executive Awareness. As part of the market assessment a brief analysis is provided for each country on the extent to which women in cybersecurity initiatives form part of the education and training market.

This market assessment chapter provides insight into the supply-side of the cybersecurity workforce ecosystem and combined with the future workforce assessment will be used to inform the gap assessment.

Summary of Market Assessment Findings

- The Market Assessment chapter examines the existing cybersecurity skills base in Cambodia, Indonesia, Mongolia, Laos and Thailand, focusing especially on gender-based opportunities to assess the current levels of female participation and accessibility.

- The chapter assesses the market on the basis of the National Cybersecurity Education capacity indicators using findings from the Strategic Drivers chapter and secondary research to capture relevant information. The indicators include evidence gathered from primary and secondary school, higher education and research, professional training and certifications and public and executive awareness offerings and initiatives.

- Research indicates that Indonesia and Thailand possess the most developed cybersecurity capacity-building programs in the region. They are also the only countries offering gender-based initiatives to address the gender gap in the sector. In both countries, military authorities and law enforcement agencies are the key providers of trainings for the public sector and knowledge for the wider public.

- All five countries have strong educational offerings. At least one university in each country offers a cyber-specific degree at both undergraduate and postgraduate level. Many more offer computer science and information technology degrees with cybersecurity modules. All examined countries, with the exception of Laos, have university-level research centres focused on cyberdefence and cybersecurity.

- Within the education sector, research did not identify any female-specific initiatives led by the universities themselves. In all countries, cybersecurity-specific education often remains the purview of the military.

- Private groups and online academies are the key providers of professional certifications. These groups provide support to both individuals and commercial entities, though they do not tailor their programmes geographically or focus on gender-based initiatives.

- Regional organisations and foreign partners are key providers of both public sector and women-focused initiatives. ASEAN, ITU, Australia, Singapore and Japan emerged as the most recurring

providers of capacity-building initiatives in the public sector. As the only non-ASEAN country in the study, Mongolia lags in this indicator. However, the OECD and the World Bank have provided and continue to provide support.

Methodology

Overview

- Research involved the review of the Strategic Drivers chapter alongside the questionnaire replies from interviews conducted earlier in the project implementation.

- Research focused on the National Cybersecurity Education capacity indicators, with special attention given to higher education and research using secondary research to capture evidence.

Sources

- Open-source resources included university websites, government websites, regional organisation websites, academic journals, newspaper articles and cybersecurity-focused data repositories.

- Key sources included but were not limited to, the Cybil Portal, the International Telecommunications Union, the Global Cybersecurity Index and ASEAN.

Key Words

- Research utilised some keywords / phrases to identify resources including but not limited to:
    - ‘’Cybersecurity’’ AND ‘’awareness’’ AND ‘’in’’ AND ‘’Southeast Asia’’
    - ‘’Cybersecurity’’ AND ‘’training’’ AND ‘’in’’ AND ‘’the’’ AND ‘’Asia Pacific’’
    - ‘’Cybersecurity’’ AND ‘’capacity building’’ AND ‘’in’’ AND ‘’Southeast Asia’’

Market Assessment Findings

Regional Efforts

Background

- In the last decade, the Asia Pacific (APAC) has faced the increasing threat of cyber-related threats and incidents.[153] While states in the region, and especially in Southeast Asia, have scaled up their cybersecurity capabilities significantly, research indicates that the five countries in the study still lack effective cyber-awareness and capability-development measures.[154] Within the context, women continue to be underrepresented in the workforce, making up less than 10 per cent of the cybersecurity workforce in APAC.[155]

- Research identified regional and international organisations, in particular ITU and ASEAN, to be key providers of cybersecurity awareness and training programs. In 2023, ITU launched its 2023/2025 regional initiative projects. Within APAC, the initiative includes, among other objectives, contributing to a secure and resilient information and communication technology environment.[156]

- ASEAN has been active in cyber capability development for the last two decades and remains a key player in both the education and the public sectors. Its programs range from the Cyber University and the Cyber SEA games, which target young adults and professionals, to strengthen cyber resilience among law enforcement in the region.[157] ASEAN is also a key facilitator of knowledge exchanges and information-sharing in the region, through joint simulations, workshops, and trainings.

- Regional and international organisations, as well as private groups, are also the main providers of female-focused initiatives in the region, with Indonesia and Thailand being the only two countries in the study to have gender-based initiatives in the sector. The UN, Australia and Microsoft emerged as significant stakeholders in increasing cyber literacy among women.

---

[153] www.pwc.com/gx/en/services/consulting/south-east-asia-consulting/digital-trust-insights-2023-southeast-asia-perspective.html

[154] www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/06/asean-cyber-security-cooperation.pdf

[155] www.asiapacific.unwomen.org/sites/default/files/Field%20Office%20ESEAsia/Docs/Publications/2020/06/Action%20Brief%20%20WPS%20%20CYBERSECURITY16620final.pdf

[156] www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/v2/2023/ITU-Asia-and-the-Pacific-Regional-Initiatives-%282023-2025%29.aspx

[157] www.aseanoer.net/main.acu ; www.facebook.com/AJCCBC/posts/pfbid02EUcRfHjRsXhgjo7M65HtU2ws2duhz5DtVs4dc1hMajfNfVTDEM4aZcPdKbAiPcdl"

Cambodia

- Cambodia scored 19.12/100 in the 2020 Global Cybersecurity Index, ranking 132nd globally and 26th regionally.[158] It is the country that scores and ranks the lowest in this research. With an internet penetration rate of 78.8 per cent in 2022, this leaves the country vulnerable to cyber threats.[159]

- Research suggests that Cambodian universities and higher education institutions offer numerous cybersecurity programs and certifications. Additionally, Cambodia has collaborated through local universities with regional and international partners to raise public and executive awareness, capacity building, as well as female-focused initiatives

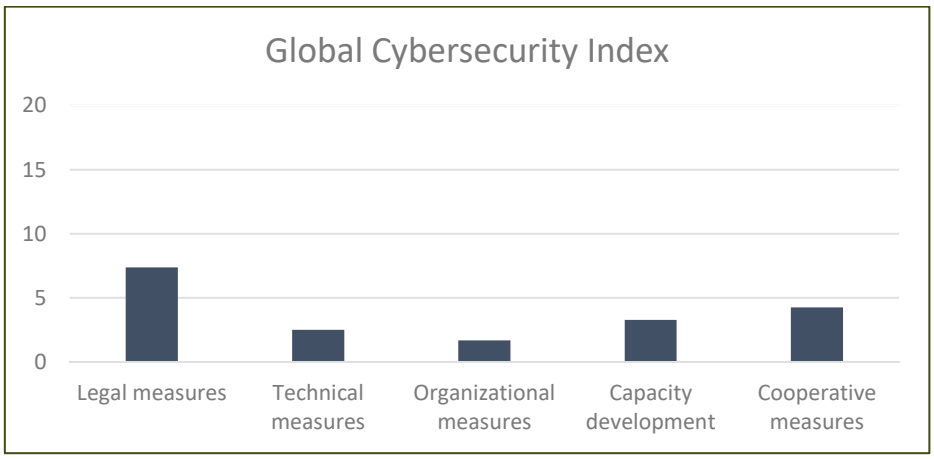


Figure 1: Global Cybersecurity Index score breakdown for Cambodia (ITU, 2020).

Existing Initiatives

Higher Education and Research

- Research points to at least four institutions offering undergraduate and graduate degrees in cybersecurity. However, many information technology and computer science programs cover cybersecurity modules within their curricula. The list below includes some examples of these but is not a comprehensive list of all relevant curricula and universities. None of the universities listed hereby advertised female-focused initiatives.

- Cambodia University of Technology and Science (CamTech) offers a bachelor's degree in cybersecurity.[160] CamTech also offers master's and doctoral degrees, but the website page is empty.[161] While it includes diversity in its values, the University does not provide statistics on the gender ratio of its researchers and student body.

- CamTech has a Cybersecurity Network Centre. Its mission is to "contribute to improve policy for strategic decision making through research, dialogue, public debate, policy

[158] www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
[159] Digital 2022: Cambodia — DataReportal – Global Digital Insights
[160] www.camtech.edu.kh/bp/
[161] www.camtech.edu.kh/masters-and-phd-programs/

engagement and training on cyber related issues."[162] The Centre also runs a program focused on cyber capacity building.[163]

- Cambodia Academy of Digital Technology offers a bachelor's degree of computer science in cybersecurity. The bachelor's degree in software engineering also covers cybersecurity modules.[164]

- The American University of Phnom Penh offers a bachelor's degree in information and communications technology, which covers network security modules.[165]

- Beltei International University offers a bachelor's degree in computer networking and cybersecurity.[166]

- University of Puthisastra offers a master's degree of science in information technology with a major in cybersecurity.[167] According to the university website, 51 per cent of the total student body and 47 per cent of the staff, are female. However, there is no breakdown per department.[168]

- The International Institute of Cambodia University of Technology offers a bachelor's and doctoral degree in computer science.[169]

- The Cambodian University of Specialties offers associate, bachelor's and master's degrees in computer science and information technology.[170]

- The University of Cambodia offers bachelor's and master's degrees in information technology, which cover cybersecurity modules.[171] The College of Science and Technology has a faculty of 17 members, of which two are women.[172]

- International University Cambodia offers a bachelor's degree in information system management and a bachelor's degree in computer science. Both degrees cover cybersecurity modules.[173]

- ASEAN Cyber University: Korea established the initiative in 2009 and has been funding it since. Seoul University implements its programs, which include the opening of e-learning

[162] www.camtech.edu.kh/cyber-security-network/
[163] www.camtech.edu.kh/cyber-security-network/
[164] www.idt.edu.kh/bachelor-of-computer-science/
[165] www.aupp.edu.kh/bachelor-of-science-in-information-and-communications-technology/
[166] www.beltei.edu.kh/biue/index.php?option=com_content&view=article&id=1029&Itemid=520
[167] www.puthisastra.edu.kh/faculty-of-business-entrepreneurship-technology/
[168] www.puthisastra.edu.kh/why-choose-up/
[169] www.iic.edu.kh/content.php?533078acd91fffef2a525239de4a3dc9=2
[170] www.cus.edu.kh/index.php?p=3
[171] www.uc.edu.kh/ucb/3/2019-08-29%2010:08:07/12/
[171] www.uc.edu.kh/ucs/Master%20Degrees/4/19/
[172] www.cost.uc.edu.kh/
[173] www.iu.edu.kh/back/en/academics/

centres in Cambodia, Laos, Thailand, Myanmar, and Vietnam. In Cambodia, the Institute of Technology of Cambodia is the main partner.[174]

Professional Training and Certification

Universities and Education Institutions:

- CamTech offers a professional diploma in cybersecurity.[175]
- American University of Phnom Penh offers a certificate course in cybersecurity.[176]
- The University of Cambodia offers an associate degree in information technology, which covers some cybersecurity modules.[177]
- Cambodia Academy of Digital Technology offers a professional certification in ethical hacking and information technology.[178]

Private and International Providers:

- Research indicates that private and international entities are the most common providers of cybersecurity trainings and certifications in Cambodia. These usually have geolocated websites for each country they operate in but offer the same curricula and programs.
- The Knowledge Academy offers certified cybersecurity professional training (CCS-PRO).[179]
- Open Development: On 04 July 2023, Open Development Cambodia hosted a cybersecurity training for civil society organisations. Of 32 participants, 12 were women.[180]
- Mildain offers a range of cybersecurity courses, including CISCO training, ethical hacking and risk and information systems control.[181]
- TopCertifier offers a certification in cybersecurity and information technology.[182]
- Unichrone offers certified information systems security professional training (CISSP).[183]

[174] www.universityworldnews.com/post.php?story=20110610213112 66 ; www.aseanoer.net/
[175] https://camtech.edu.kh/pdp/
[176] https://www.aupp.edu.kh/certificate-courses/cybersecurity-certificate-course/
[177] www.uc.edu.kh/ucs/Associate%20Degrees/4/17/
[178] www.idg.edu.kh/professional-training-programs/
[179] www.theknowledgeacademy.com/kh/courses/cyber-security-training/
[180] www.opendevelopmentcambodia.net/cybersecurity-training/
[181] www.mildaintrainings.com/loc/cyber-security-training-in-cambodia/
[182] www.iso-certification-cambodia.com/cyber-security-certification.html
[183] www.unichrone.com/kh/cissp-certification-training

- Step It academy runs courses on cybersecurity essentials.[184] Step It also set up the first female coding club in Cambodia, Sisters of Code, which offers CS training for female high school students. [185]

Public and Executive Awareness

National initiatives:

- CamTech: On 12 January 2023, CamTech held an interactive workshop titled, "Cyber Essentials – be digitally ready to reduce your risks". The workshop targeted civil servants from a range of ministries, with the aim of acquainting them with internet and data protection basics. The National Institute of Science technology and Innovation, the Asian Vision Institute, and the Foreign Ministry collaborated in the organisation of the event.[186]

- Cambodia Academy of Digital Technology: The Institute of Digital Governance within the Academy offers digital governance trainings, including CISCO certifications, for civil servants and state employees.[187]

- Telecommunication Regulator of Cambodia (TRC) and Securities and Exchange Regulator of Cambodia (SERC): On 31 May 2023, the two regulators held a capacity building training on cybersecurity for SERC officials. The training focused on the increase in cybercrime in the country, and prevention mechanisms SERC officials can use to mitigate cyber threats.[188]

- Cambodia Computer Emergency Response Team (CERT) and Ministry of Posts and Telecommunications: In 2017 the Department of ICT at the Ministry and CERT started running an annual cyber exercise called Cyber Angkor.[189] Alongside this initiative, the two bodies also routinely host trainings and seminars for civil servants. For example, one of the latest ones, held on 22 May 2022, covered cyber incident response essentials.[190]

Regional and international initiatives:

- United Nations:
    - **Regional Framework towards Peaceful, Inclusive Societies**: The UN Women Regional Office for Asia and the Pacific developed the framework with the aim of including women in sustainable governance and peace-building processes, allowing them to benefit from sustained peace and gender-responsive laws.

[184] www.cambodia.itstep.org/cyber-security
[185] www.sistersofcode.org
[186] www.camtech.edu.kh/wp-content/uploads/2022/12/Outline-Cyber-Essentials-Workshop12-01-2023-3-3.pdf
[187] www.idg.edu.kh/cisco-academy/
[188] www.eacnews.asia/home/details/22982
[189] www.camcert.gov.kh/cyber-angkor-2017/
[190] www.camcert.gov.kh/workshop-on-cybersecurity-and-cyber-incident-response-essentials/

Within the first outcome, the framework includes provisions for increased presence of women in emerging areas, including cybersecurity.[191]

- **Women in International Security and Cyberspace Fellowship**: The United National Institute for Training and Research established the fellowship in 2019, with funding from Australia, the US, UK, Canada, the Netherlands, and New Zealand. The Fellowship aims to train female diplomats from numerous regions, including East Asia, who participate at the United National cyber negotiations. The project seeks to upskill them in cyber governance matters, while ensuring equal and effective representation at the negotiations table.[192]

- Asia Pacific Internet Development Fund (APIDIT):
  - **Supporting Women in Technical and Research Project (Switch):** APIDIT and the Asia Pacific Network Information Centre kickstarted Switch in June 2022. The project seeks to support the career development of women and LGBTQI+ persons working on internet development. It provides them with technical training, professional certifications, and mentoring services, with the aim of expanding their professional network and expanding the role of women and the LGBTQI+ community in information technology and cybersecurity.[193] The project builds upon the Switch Sea initiative, funded, and implemented by Australia and described below.

- Association of Southeast Asian Nations (ASEAN):
  - **ASEAN Cyber Capacity Program (ACCP):** The program, established in 2016 by Singapore, aims to build cyber capacity in ASEAN members.[194] Upon its establishment in 2016, Singapore allocated over USD 7 million funding for an initial five years. ACCP has since been renewed. The program targets a wide audience, ranging from diplomats to technical operators and analysts. The ACCP includes a series of workshops and seminars, as well as the ASEAN Ministerial Conference on Cybersecurity.[195]

  - **ASEAN-Singapore Cybersecurity Centre for Excellence (ASCCE):** ASCCE is linked to the ACCP. It extends the scope of the program to include trainings on cyber-legislation development, information sharing among Computer Emergency Response Teams (CERTS), and cooperation with non-ASEAN members, including Korea, Australia, the US, and UK, in designing cyber capacity-building programs.[196]

---

[191] www.asiapacific.unwomen.org/en/digital-library/publications/2023/05/advancing-the-women-peace-and-security-agenda-and-inclusive-governance
[192] www.thegfce.org/women-in-international-security-and-cyberspace-fellowship/
[193] www.cybilportal.org/projects/switch-supporting-women-in-technical-and-research-project/
[194] www.csa.gov.sg/docs/default-source/csa/documents/sicw-2016/factsheet_accp_final.pdf?sfvrsn=a45aecbb_0#:~:text=Cyber%20Capacity%20Programme-,The%20ASEAN%20Cyber%20Capacity%20Programme%20(ACCP)%20aims%20to%20build%20cyber,secure%20and%20resilient%20ASEAN%20cyberspace.
[195] www.cybilportal.org/projects/asean-cyber-capacity-programme-accp/
[196] www.cybilportal.org/projects/asean-singapore-cybersecurity-centre-for-excellence-ascce/

- **ASCCE-UK Digital Diplomacy Course**: The Singapore Cybersecurity Agency and the UK Foreign, Commonwealth and Development Office jointly funded and implemented the course in September 2022. The project sought to educate ASEAN policy makers on cybersecurity and digital security matters.[197]

- **Third Country Training Program**: The Singaporean Ministry of Foreign Affairs and the United States Department of State have been running cybersecurity workshops for ASEAN members since 2016. The program, implemented by the US Department of Homeland Security, consists of a yearly workshop where ASEAN member states share best practices on cybersecurity development.[198]

- **ASEAN Cyber Capacity Development Project**: The Japan-ASEAN integration Fund funded the project, while Interpol implemented it. The project, which ran from January 2016 to December 2021, focused on building the capabilities of ASEAN member states to fight cybercrime.[199]

- Australia:
  - **Supporting Women in Internet Research Leaders in Southeast Asia (Switch Sea):** The Australian Department of Foreign Affairs and Trade (DFAT) implemented the project from May 2020 to December 2021 with the aim of fostering diversity and gender empowerment within the internet industry in Southeast Asia. The project started with a cohort of 100 women and LGBTQI+ engineers, providing them with education, training and mentoring in both technical and leadership matters.[200]

  - **International Law in the Cyber Era:** From May 2020 to July 2021, Cyber Law International, with the financial support from DFAT, delivered this program. The project focused on the links between human rights and cybersecurity, including the management of harmful content online, online surveillance, and risks associated with e-provision of public services.[201]

  - **Cambodian Cybersecurity Uplift**: DFAT funded the project, while CyberCX implemented it. The program ran from June 2021 to June 2022. Themes and topics incused cybersecurity policy and strategy covering norms and cyber-

[197] www.cybilportal.org/projects/ascce-uk-digital-diplomacy-course/
[198] www.cybilportal.org/projects/singapore-united-states-third-country-training-programme-tctp-cybersecurity-workshops/
[199] www.cybilportal.org/projects/asean-cyber-capacity-development-project/
[200] www.cybilportal.org/projects/switch-sea-fostering-womens-technical-leadership-in-the-internet-industry-in-southeast-asia/
[201] www.cybilportal.org/projects/international-law-in-the-cyber-era-finding-balance-between-state-interests-and-individual-rights-asia-pacific/

diplomacy and cybersecurity culture and skills covering education, training & workforce development[202]

-
    - **Cyber Bootcamp for Cambodia:** Training activities on Cyber Bootcamp for Cambodia, which Australia has cooperated with Cambodia 3 times to conduct the training from 2021 to 2023 in aims to strengthen the cyber security capacity of stakeholders in Cambodia to be prepared in advance to manage, prevent and respond to digital security issues effectively and timely.[203]

    - **Strengthening Digital Media Literacy in the Mekong:** DFAT funded the project, while the International Foundation for Electoral systems implemented it. The program targeted women, minorities, and vulnerable populations with the aim of strengthening their digital media literacy, and their ability to recognise and counter harmful content online.[204]

- United States:
    - **USAID Digital Asia Accelerator (DAA):**
        - USAID, Development Alternatives Incorporated (DAI) and the US Department of State launched the project in September 2019, with the aim of improving digital skills across Southeast Asia, among other objectives.
        - DAA includes the Cyber for Her: Upskilling and Competition (August 2023) which aims to attract and empower women to pursue and advance careers in the field of Cybersecurity, and the Women's Digital Inclusion Challenge, which is set to digitally upskill women entrepreneurs and women-led businesses in cybersecurity, and digital economy matters.[205]
        - In 2021, the DAA launched the Cambodia SME Digital Upskilling program to help SMEs access and use safe digital tools.[206]
        - In 2022, the DAA also launched the Developing Cybersecurity Reporting Expertise for Female Journalists in Asia and the Pacific Program which focused on the importance of the media in promoting digital safety.[207]

    - **The Cyber Capabilities and Capacity Development Project (C3DP)** is a two-year project funded by the Bureau of International Narcotics and Law Enforcement Affairs and implemented by Interpol. It aims to develop the capabilities of law

[202] www.cybilportal.org/projects/cambodian-cyber-security-uplift-cyber-security-capability-assessment/ ; https://cybilportal.org/projects/cambodian-cyber-security-uplift-cyber-security-training/
[203] https://www.camcert.gov.kh/cyber-bootcamp-cambodia-2023/
[204] www.ifes.org/programs-initiatives/strengthening-digital-media-literacy-mekong-region ; www.cybilportal.org/projects/strengthening-digital-media-literacy-in-the-mekong/
[205] www.usaid.gov/sites/default/files/2023-05/Digital%20Asia%20Accelerator%20Factsheet_1.pdf
[206] https://concoursn.com/dai-announces-call-for-innovative-solutions-to-advance-digital-skills-for-small-firms-cambodia/
[207] https://www.linkedin.com/posts/asia-pacific-institute-for-broadcasting-development_happy-international-womens-day-2023-theme-activity-7039077437573406720-w8Ov/?originalSubdomain=lk

enforcement agencies in Southeast Asia to combat cyber-crime. The project also establishes Regional Expert Groups to facilitate knowledge exchanges.[208]

- Japan:
    - The Japan international Cooperation Agency has funded and implemented the Project for Improvement of Cyber Resilience in Cambodia. The project targets the Department of ICT at the Ministry of Post and Telecommunications with the aim of improving its cybersecurity capabilities and helping Cambodia achieve Sustainable Development Goals 9 and 17.[209]

    - Grant Aid for the "Economic and Social Development" programme in November 2022, executed under the Ministry of Foreign Affairs (MOFA) of Japan.[210]

    - Grant on the construction and equipment necessary for the National Data Center. The ground-breaking ceremony for the National Data Center in Phnom Penh took place in July 2023. The center is expected to be fully operational by 2025 and will serve as a centralized hub for storing and processing data for the Cambodian government.[211]

- ICT4Peace Foundation:
    - Between 2014 and 2018, ICT4Peace ran an international cybersecurity capacity building program that targeted Cambodia, among other countries. The program dealt with a wide range of cybersecurity-related topics, including international cooperation in cybersecurity matters, national cybersecurity strategy building, and the establishment of CERTS.[212]

Women in Cybersecurity

- Research shows that Cambodian universities and higher education institutions do not offer gender-based programs, whether in the form of scholarships or special recruitment efforts. They also do not publish gendered statistics of their student body.

- International partners and regional organisations are the only entities to provide female-focused and gender-based training programs. However, these mostly target the public sector and civil servants, indicating a potential gap in the private sector.

[208] www.cybilportal.org/projects/cyber-capabilities-and-capacity-development-project-c3dp/
[209] www.jica.go.jp/Resource/english/news/press/2022/20221205_41.html#:~:text=In%20order%20to%20improve%20the,for%20the%20general%20public%2C%20and
[210] https://mfaic.gov.kh/files/uploads/B5WJMWGIAW70/ENG_PR_Signing%20with%20JP.pdf
[211] https://w.media/japan-commits-16-million-grant-aid-to-cambodia-for-national-data-center/
[212] www.ict4peace.org/wp-content/uploads/2018/09/Outline-Capacity-Building-20180827.pdf

Indonesia

- Indonesia scored 94.88 /100 in the 2020 Global Cybersecurity Index, ranking 23rd globally and 6th regionally.[213] It is the country that scores and ranks the highest in this research, both in terms of global score and capacity development initiatives.

- Indonesia presents a wide array of cybersecurity capacity building initiatives, mostly led by the government, which target high school and university students, as well as civil servants and government officials. It also partakes in ASEAN and other regional initiatives.

- Indonesia has gender-based programs to encourage female participation in the cyber sector at both educational and professional levels. The National Cyber and Crypto Agency (BSSN) has also openly recognised the importance of women in cybersecurity.[214]

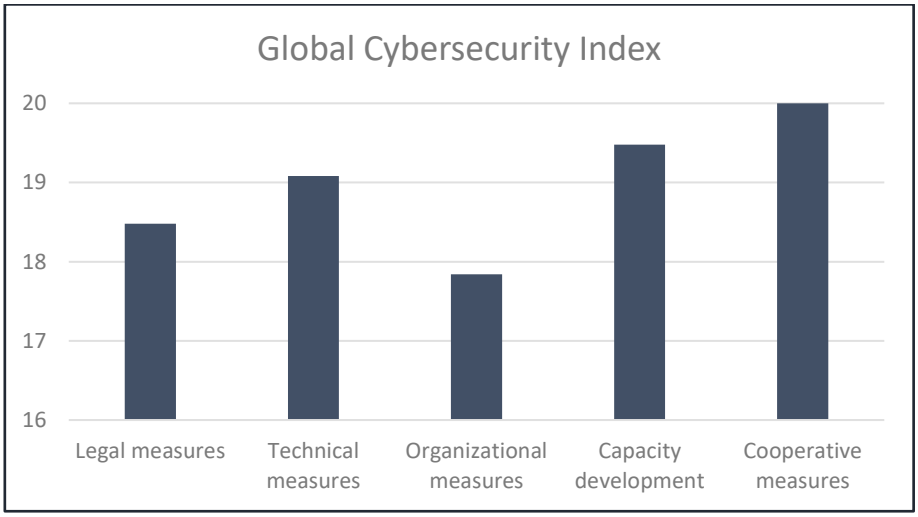


Figure 2: Global Cybersecurity Index score breakdown for Indonesia (ITU, 2020).

Existing Initiatives

Primary and Secondary School

- National Cyber and Crypto Agency (BSSN): In October 2022, the BSSN launched the #JagaRuangSiber campaign with the aim of increasing cybersecurity awareness among high school students.[215] It is worth noting that the BSSN website displays an education and literacy tab, where they provide cybersecurity awareness tips and information. Many of the articles tackle topics such as child safety online.[216]

Higher Education and Research

[213] www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
[214] www.en.antaranews.com/news/281928/women-have-vital-role-in-cybersecurity-bssn
[215] www.jakartadaily.id/tech-media/pr-1625515091/bssn-campaigns-for-cyber-security-cultural-literacy-among-highschool-students-with-jagaruangsiber-program
[216] www.bssn.go.id/masyarakat-umum/ ; https://www.bssn.go.id/publikasi/

- Research points to at least five institutions offering undergraduate and graduate degrees in cybersecurity. However, many information technology and computer science programs cover cybersecurity modules within their curricula. The list below includes some examples of these, but is not a comprehensive list of all relevant curricula and universities. According to a paper published by Telkom University, Indonesian university students have a good awareness of cybersecurity.[217] The list below includes some examples of these. Research did not identify any women-focused initiatives within Indonesian universities.

- Binus University offers a bachelor's degree in cybersecurity.[218]

- Telkom University offers a bachelor's degree of information technology with concentrations in cybersecurity and Internet of things.[219] The University also offers a master's degree in cybersecurity and digital forensics. The academic coordinator for the program is a woman.[220] The School of Informatics also has a Cyber Physical Systems Expertise Group in the faculty, and it offers a doctoral degree on the subject.[221]

- The Bandung Institute of Technology also hosts the Centre for Defence and Security Technology. The Centre conducts research and development to develop both products and human resources on the matter.[222]

- The Bandung Institute of Technology offers a bachelor's degree Informatics Engineering, which includes some security modules.[223] It also offers a master's degree in informatics, where students can then specialise in cybersecurity.[224] The faculty has several research groups, including one in Computer Engineering and Informatics, which focus on computer network security, among other topics.[225]

- Monash Indonesia offers a master's degree in cybersecurity.[226]

- Monash Indonesia also has a PhD programme in cybersecurity. Research focuses on secure AI-enhanced light curve analysis for satellite detection in space surveillance cybersecurity and on privacy-preserving artificial intelligence in smart city context surveillance.[227]

- The University of Indonesia offers a bachelor's degree of Computer Science, which also covers cybersecurity courses.[228] The university also offers masters and doctoral degrees within the faculty of computer science, though neither openly mention cybersecurity modules.

---

217 www.researchgate.net/publication/347111955_Analysis_of_College_Students'_Cybersecurity_Awareness_In_Indonesia

218 www.curriculum.binus.ac.id/program/cyber-security/

219 www.bit.telkomuniversity.ac.id/

220 www.msf.telkomuniversity.ac.id/

221 www.telkomuniversity.ac.id/en/school-of-informatics/

222 www.itb.ac.id/center-for-defense-and-security-technology

223 www.stei.itb.ac.id/en/undergraduate-programs/bachelor-informatics/

224 www.stei.itb.ac.id/en/postgraduate-programs/master-of-informatics-engineering/

225 www.stei.itb.ac.id/en/research-groups/

226 www.monash.edu/study/courses/find-a-course/indonesia-course/master-of-cybersecurity-c6010

227 www.monash.edu/indonesia/our-programs/doctor-of-philosophy-phd/Monash-Indonesia-Inspire-Doctoral-Scholarship-Program

228 www.ui.ac.id/en/academic/faculty/faculty-of-computer-science/

- University Gadjah Mada offers a bachelor's degree in information engineering, with a module in computer network security as well as security and data integrity.[229] The university also offers an Information Technology Masters, with a concentration in network and cybersecurity.[230]

- Universitas Airlangga offers a bachelor's degree in information systems, with an information systems security module which covers cybersecurity.[231]

- Jakarta Negeri Polytechnic has a diploma in Computer and Networking Engineering, which covers cybersecurity modules.[232]

- State Cyber and Crypto Polytechnic (SSN) hosts the Cybersecurity Engineering scientific group. The SSN has a Research Laboratory with four scientific groups, including the Cybersecurity Engineering one, where students and lecturers can conduct research.[233]

- SSN Polytechnic: On 25 August 2023, the SSN Polytechnic and the BSSN held an International Conference on Cryptography, Informatics and Cybersecurity. The institutions noted that they organised the event with the aim of supporting research in cybersecurity and cryptography, with a mixed audience of academics, students and practitioners attending.[234]

Professional Training and Certification

Universities and Education Institutions:

- SSN Polytechnic offers an associate degree (vocational training equivalent) in cybersecurity.[235]

- Ministry of Communication and Informatics: In 2018, the Ministry and the EC-Council set up the Digital Talent Scholarship Program. The program offers 1,000 scholarships to young graduates to get cybersecurity training certifications.[236]

Private and International Providers:

- Research identified several private, non-state organisations and international partners that provide cybersecurity trainings and certifications in Indonesia. Among the private providers, several are international websites that provide country-specific courses.

- Sans offers cybersecurity training events and enterprise penetration testing courses.[237]

[229] www.sarjana.jteti.ugm.ac.id/undergraduate-program/information-engineering-undergraduate/curriculums/
[230] www.pasca.jteti.ugm.ac.id/2022/10/12/program-studi-magister-teknologi-informasi/
[231] www.si.fst.unair.ac.id/kurikulum/
[232] www.tik.pnj.ac.id/readmore/5e2016a01c6cc70c3069babf/d1-teknik-komputer-dan-jaringan
[233] www.poltekssn.ac.id/en/penelitian-dan-pengabdian-masyarakat/
[234] www.bssn.go.id/politeknik-siber-dan-sandi-negara-bssn-selenggarakan-international-conference-on-cryptography-informatics-and-cybersecurity-icocics-2023/
[235] www.poltekssn.ac.id/en/rekayasa-keamanan-siber/
[236] www.eccouncil.org/ec-council-in-news/ec-council-collaborates-with-indonesias-ministry-of-communication-and-informatics-to-facilitate-cybersecurity-training/
[237] www.sans.org/cyber-security-training-events/indonesia-2023/

- SkillLogic offers a cybersecurity certification course.[238]

- NobleProg offers a range of courses, including Cipher Trust Manager, Cybersecurity with Python, CCTV Security, Security Management, Cloudflare Essentials, Honeywell Security System, Cybersecurity Awareness Training, Open Authentication, Synk and OpenStack Security courses.[239]

- SimpliLearn offers an online Postgraduate program in cybersecurity.[240]

- The Australia-Indonesia Centre runs cybersecurity skills training for micro, small and medium enterprises (MSMEs). The course focuses on basic cybersecurity competencies to increase e-commerce capabilities of MSMEs. DFAT funds the program, which the BSSN and the Indonesian Ministry of Cooperation then implement. While the program does not target women directly, the MSME focus means that many of the beneficiaries are women.[241]

- The Japan International Cooperation Agency (JICA) runs the Project for Human Resources development for Cybersecurity Professionals. JICA funds the project, which the University of Indonesia and the Ministry of Communication and Information Technologies implement. The course aims to upskill cybersecurity professionals.[242]

- ISACA Indonesia Chapter offers Certification for Information Security Managers courses. The certification focuses on information security governance, information security risk management, information security program and incident management.[243] ISACA also offers other certifications including trainings for information systems auditors, risk and information systems control, data privacy solutions engineers and governance of enterprise IT.[244]

- Open Web Application Security Project (OWASP) Indonesia chapter runs trainings on ransomware and penetration testing. The courses are free and accessible to all interested individuals.[245]

Public and Executive Awareness

National initiatives:

- University of Indonesia: The University hosts and runs a digital resilience and cybersecurity academy for government officials. The University runs trainings and

[238] www.skillogic.com/cyber-security-certification-course-indonesia/
[239] www.nobleprog.id/cybersecurity-training
[240] www.simplilearn.com/pgp-cyber-security-certification-training-course-in-jakarta-city
[241] www.skills.australiaindonesiacentre.org/news/cyber-security-course-helps-indonesian-small-business-2/ ; www.skills.australiaindonesiacentre.org/news/e-commerce-cybersecurity-for-msmes-in-indonesia-information-and-faqs/
[242] www.cybilportal.org/projects/project-for-human-resources-development-for-cyber-security-professionals/
[243] www.isaca.org/credentialing/cism
[244] www.isaca.org/credentialing
[245] www.owasp.org/www-chapter-jakarta/

workshops for both trainers and government officials, on topics ranging from online and offline security, e-governance and cybersecurity and digital forensics. The website is currently advertising one that will take place on 28 November 2023.[246]

  - On 06 November 2020, the university held a 5-part teaching training on gender awareness in cybersecurity and the gender divide in the field. The course aimed to improve gender awareness, covering topics such as gender and cybercrime, gender and law and the digital gender divide.[247]

- Indonesia Women in Cybersecurity (IWCS): Indonesian female cybersecurity practitioners set up IWCS in 2021, with the aim of increasing women's participation in the cyber sector. The website advertises education as one of their pillars and they also have mentorship and apprenticeship programs.[248]

Regional and international initiatives:

- United Nations:
  - **Regional Framework towards Peaceful, Inclusive Societies:** The UN Women Regional Office for Asia and the Pacific developed the framework with the aim of including women in sustainable governance and peace-building processes, allowing them to benefit from sustained peace and gender-responsive laws. Within the first outcome, the framework includes provisions for the increased presence of women in emerging areas, including cybersecurity.[249]

  - **Women in International Security and Cyberspace Fellowship:** The United National Institute for Training and Research established the fellowship in 2019, with funding coming from Australia, the US, UK Canada, the Netherlands and New Zealand. The Fellowship aims to train female diplomats from numerous regions, including East Asia, who participate at the United National cyber negotiations. The project seeks to upskill women in cyber governance matters, while ensuring equal and effective representation at the negotiations table.[250]

- Association of Southeast Asian Nations (ASEAN):
  - **ASEAN Cyber Capacity Program (ACCP):** The programs established in 2016 by Singapore, aims to build cyber capacity in ASEAN members.[251] Upon its establishment in 2016, Singapore allocated over USD 7 million funding for an initial five years. ACCP has since been renewed. The program targets a wide

[246] www.law.ui.ac.id/digital-resilience-and-cyber-security-academy-training-of-trainers-digital-resilience-and-cyber-security-academy-for-government-officials/
[247] https://law.ui.ac.id/cyber-cyber-security-education-in-indonesia-through-a-multidisciplinary-approach-of-study-programs-and-innovative-technologies-2/
[248] https://iwcs.id/about-us/
[249] www.asiapacific.unwomen.org/en/digital-library/publications/2023/05/advancing-the-women-peace-and-security-agenda-and-inclusive-governance
[250] www.thegfce.org/women-in-international-security-and-cyberspace-fellowship/
[251] www.csa.gov.sg/docs/default-source/csa/documents/sicw-2016/factsheet_accp_final.pdf?sfvrsn=a45aecbb_0#:~:text=Cyber%20Capacity%20Programme-,The%20ASEAN%20Cyber%20Capacity%20Programme%20(ACCP)%20aims%20to%20build%20cyber,secure%20and%20resilient%20ASEAN%20cyberspace.

audience, ranging from diplomats to technical operators and analysts. The ACCP includes a series of workshops and seminars, as well as the ASEAN Ministerial Conference on Cybersecurity.[252]

- **ASEAN-Singapore Cybersecurity Centre for Excellence (ASCCE):** ASCCE is linked to the ACCP. It extends the scope of the program to include trainings on cyber-legislation development, information sharing among Computer Emergency Response Teams (CERTS), and cooperation with non-ASEAN members, including Korea, Australia, the US, and the UK in designing cyber capacity-building programs.[253]

- **ASCCE-UK Digital Diplomacy Course**: The Singapore Cybersecurity Agency and the UK Foreign, Commonwealth and Development Office jointly funded and implemented the course in September 2022. The project sought to educate ASEAN policy makers on cybersecurity and digital security matters.[254]

- **Third Country Training Program:** The Singaporean Ministry of Foreign Affairs and the United States Department of State have been running cybersecurity workshops for ASEAN members since 2016. The program, implemented by the US Department of Homeland Security, consists of a yearly workshop where ASEAN member states share best practices on cybersecurity development.[255]

- **ASEAN Cyber Capacity Development Project:** The Japan-ASEAN integration Fund funded the project, while Interpol implemented it. The project, which ran from January 2016 to December 2021, focused on building the capabilities of ASEAN member states to fight cybercrime.[256]

- **Building Anti-Cybercrime Capacity in ASEAN Through Simulation Exercises:** Canada funded the project, which ended in March 2023. The initiative set up bilateral simulation exercises, as well as a regional one, with the aim of testing preparedness to cyber incidents.[257]

- Australia:
  - **International Law in the Cyber Era**: From May 2020 to July 2021, Cyber Law International, with the financial support of DFAT, delivered a project focused on the links between human rights and cybersecurity. The project included the management of harmful content online, online surveillance and risks associated with e-provision of public services.[258]

[252] www.cybilportal.org/projects/asean-cyber-capacity-programme-accp/
[253] www.cybilportal.org/projects/asean-singapore-cybersecurity-centre-for-excellence-ascce/
[254] www.cybilportal.org/projects/ascce-uk-digital-diplomacy-course/
[255] www.cybilportal.org/projects/singapore-united-states-third-country-training-programme-tctp-cybersecurity-workshops/
[256] www.cybilportal.org/projects/asean-cyber-capacity-development-project/
[257] www.cybilportal.org/projects/building-anti-cybercrime-capacity-in-asean-through-simulation-exercises/
[258] www.cybilportal.org/projects/international-law-in-the-cyber-era-finding-balance-between-state-interests-and-individual-rights-asia-pacific/

- United States:
    - **USAID Digital Asia Accelerator (DAA):**
        - USAID, Development Alternatives Incorporated (DAI) and the US Department of State launched the project in September 2019, with the aim of improving digital skills across Southeast Asia, among other objectives.
        - DAA includes the Cyber for Her: Upskilling and Competition (August 2023) which aims to attract and empower women to pursue and advance careers in the field of Cybersecurity, and the Women's Digital Inclusion Challenge, which is set to digitally upskill women entrepreneurs and women-led businesses in cybersecurity, and digital economy matters.[259]
        - In 2021, the DAA launched the USAID JAPRI Digital Literacy Training Program which aims to help young entrepreneurs which included young aspiring women across East Java, Indonesia grow their businesses safely online. The DAA partnered with WhatsApp for Business and Microsoft to develop a tailored curriculum that addresses specific gaps and needs of the communities.[260]
        - In 2022, the DAA also launched the Developing Cybersecurity Reporting Expertise for Female Journalists in Asia and the Pacific Program which focused on the importance of the media in promoting digital safety.[261]

    - The **Cyber Capabilities and Capacity Development Project (C3DP)** is a two-year project funded by the Bureau of International Narcotics and Law Enforcement Affairs and implemented by Interpol. It aims to develop the capabilities of law enforcement agencies in Southeast Asia to combat cyber-crime. The project also establishes Regional Expert Groups to facilitate knowledge exchanges.[262]

    - **International Program on Cybersecurity Studies (iPCSS):** The program, funded by the United States and Germany, aims to train senior government officials to better deal with transnational cybersecurity challenges. It also tackles cybersecurity policy development and its implementation.[263]

    - The US cybersecurity and infrastructure agency also ran a **cyber hygiene workshop** with the Indonesian BSSN and the Thai NSCA on 21 April 2023.[264] The workshop focused on information technology/operational technology (IT/OT), industrial control systems, threat actors, threat intelligence, cyber-attack frameworks, workforce development tools, and case studies of common attacks.

[259] www.usaid.gov/sites/default/files/2023-05/Digital%20Asia%20Accelerator%20Factsheet_1.pdf
[260] https://www.youtube.com/watch?v=Tv-wXPx9CbA; https://pdf.usaid.gov/pdf_docs/PA00Z5WZ.pdf
[261] https://www.linkedin.com/posts/asia-pacific-institute-for-broadcasting-development_happy-international-womens-day-2023-theme-activity-7039077437573406720-w8Ov/?originalSubdomain=lk
[262] www.cybilportal.org/projects/cyber-capabilities-and-capacity-development-project-c3dp/
[263] www.cybilportal.org/projects/cyber-security-assistance-international-program-on-cyber-security-studies-ipcss/
[264] www.cisa.gov/news-events/news/cisa-building-cyber-hygiene-capacity-thailand-philippines-and-indonesia

- United Kingdom:
    - **CybHER initiative**: The British Embassy in Jakarta runs cybersecurity and cyber hygiene courses for women —comprising of students, young professionals, and female leaders of micro, small and medium enterprises (MSMEs). The courses are focused on e-commerce with the aim of reducing cyber threats that women face in their MSMEs.[265]
    - **Get Safe Online Indonesia**: The UK funded the project via the Digital Access Program. Get Safe Online is a website to educate citizens on cyber hygiene and security matters. It covers good practices for computers, smartphones, and tablets, fintech services, social networks, and safeguarding children. [266]
    - **Trust and Resilience Digital Access Program**: The program, which ended in March 2023, aimed to increase national cybersecurity capacity and resilience to cybersecurity threats. To do so, it provided government-to-government technical assistance, as well as cyber hygiene training, public awareness-raising, and research initiatives.[267]
- Japan:
    - **Countermeasures against cybercrime:** Tokyo funded the initiative – which ended in December 2015 – and the Japan International Cooperation Agency implemented it. The Agency provided Indonesian police forces and other legal bodies with trainings on the Japanese experience with cybercrime and the measures the country has put in place to reduce and combat it.[268]
- Microsoft:
    - **Cybersecurity Skills Initiative**: Through the initiative, Microsoft delivers grants to non-profits to help skill people for the cybersecurity workforce.[269]
    - **Microsoft Women@Cybersecurity**: In April 2022, Microsoft and the BSSN hosted the event, with the aim of familiarising high school and university girls with careers in cybersecurity.[270]

Women in Cybersecurity

- Research shows that at least two Indonesian institutions – the University of Indonesia, and the BSSN – have implemented gender-based programs. While both initiatives were limited in scope and reach as they only captured women in the public sector, the initiative highlights the awareness of the importance of closing the digital gender divide to some degree. Future initiatives should consider women in other sectors in order to have a wider reach.

[265] www.jakartaglobe.id/tech/uk-helps-indonesia-empower-women-with-cybersecurity-skills
[266] www.getsafeonline.id/en/ ; https://cybilportal.org/projects/indonesia-cyber-awareness-bilingual-website/
[267] www.cybilportal.org/projects/digital-access-programme-trust-resilience/
[268] www.cybilportal.org/projects/countermeasures-against-cybercrime/
[269] www.blogs.microsoft.com/on-the-issues/2023/04/19/cybersecurity-skills-initiative-expansion-nonprofits/
[270] https://news.microsoft.com/th-th/2022/04/19/women-cybersecurity-en/

- Indonesia remains reliant on international organisations and foreign partners for women-facing initiatives, with the UK, Australia and the US being the top providers.

Laos

- Laos scored 20.34/100 in the 2020 Global Cybersecurity Index, ranking 131st globally and 25th regionally.[271] It is the second lowest-scoring country in the study after Cambodia. Laos is also the country with the lowest internet penetration rate in the cohort, which stood at 62 per cent at the start of 2023.[272]

- Research indicates that, as was the case with Cambodia and Indonesia, universities in Laos offer both cybersecurity degrees and degrees in tangential subjects, with cybersecurity modules. The list below includes some examples of these, but is not a comprehensive list of all relevant curricula and universities. It is worth emphasising here that many Laotian universities have outdated or inaccessible websites, which restricted the scope of research.

- Regarding public and executive awareness, as well as female-focused initiatives, the country seems to mostly rely on regional and international initiatives. It is expected that Laos will ramp up its cybersecurity capacity in the coming years, in concomitance with the 2021-2024 National Digital Economic Development Vision.[273]

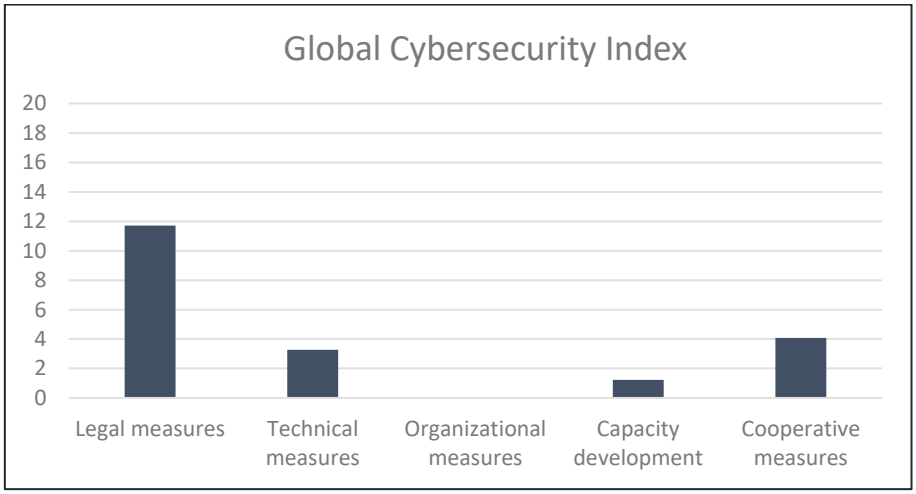


Figure 3: Global Cybersecurity Index score breakdown for Laos (ITU, 2020).

Existing Initiatives

[271] www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
[272] www.datareportal.com/reports/digital-2023-laos#:~:text=There%20were%204.70%20million%20internet%20users%20in%20Laos%20in%20January,percent)%20between%202022%20and%202023.
[273] www.greatermekong.org/g/lao-pdr-prime-minister-urges-development-country%E2%80%99s-digital-pillars#:~:text=Lao%20PDR%20is%20implementing%20the,Development%20Plan%20for%202021%2D2025

Primary and Secondary School

- Lao Computer Incident Response Team (CERT): The team organises cyber competitions and hacking games open to ages 13-29.[274]

Higher Education and Research

- National University of Laos offers a bachelor's degree in information technology with a cybersecurity concentration.[275]

- Lao Korean College offers a bachelor's degree in computer science with cybersecurity modules.[276]

- Korea established the ASEAN Cyber University in 2009 and has been funding it since. Seoul University implements its programs, which include the opening of e-learning centres in Cambodia, Laos, Thailand, Myanmar, and Vietnam.[277]

Professional Training and Certification

National initiatives:

- Lao CERT: cybersecurity and online safety training courses.[278] The CERT website advertises the courses and routinely publishes articles and information about safety online and cybersecurity basics.[279]

Private and International Providers:

- Research indicates that private and international entities are the most common providers of cybersecurity trainings and certifications in Laos. These usually have geolocated websites for each country they operate in but offer the same curricula and programs.

- The Knowledge Academy offers a Cybersecurity Awareness Course.[280]

- Unichrone offers CISSP Certification Trainings.[281]

- Mildain offers Cybersecurity Certification Trainings, among other subjects.[282]

Public and Executive Awareness
National initiatives:

[274] www.laocert.gov.la/activity/24
[275] www.fe-nuol.edu.la/en/computer-engineering-and-it/
[276] www.lkclaos.org/department-of-computer-science/
[277] www.universityworldnews.com/post.php?story=20110610213112 66 ; www.aseanoer.net/
[278] www.laocert.gov.la/pages/3
[279] www.laocert.gov.la/articles/65
[280] www.theknowledgeacademy.com/la/courses/cyber-security-training/cyber-security-awareness/
[281] www.unichrone.com/la/cissp-certification-training/vientiane
[282] www.mildaintrainings.com/loc/cyber-security-training-in-laos/

- Lao CERT runs cybersecurity and e-governance workshops and trainings for civil servants and public sector employees.[283] For example, in February 2020, they ran one on network and information security management.

Regional and international initiatives:

- United Nations:
    - **Regional Framework towards Peaceful, Inclusive Societies**: The UN Women Regional Office for Asia and the Pacific developed the framework with the aim of including women in sustainable governance and peace-building processes and allowing them to benefit from sustained peace and gender-responsive laws. Within the first outcome, the framework includes provisions for increased presence of women in emerging areas, including cybersecurity.[284]

    - **Women in International Security and Cyberspace Fellowship**: The United National Institute for Training and Research established the fellowship in 2019, with funding coming from Australia, the US, UK, Canada, the Netherlands and New Zealand. The Fellowship aims to train female diplomats from numerous regions, including East Asia, who participate at the United National cyber negotiations. The project seeks to upskill them in cyber governance matters, while ensuring equal and effective representation at the negotiations table.[285]

- Asia Pacific Internet Development Fund (APIDIT):
    - **Supporting Women in Technical and Research Project (Switch):** APIDIT and the Asia Pacific Network Information Centre kickstarted Switch in June 2022. The project seeks to support the career development of women, and LGBTQI+ persons working on internet development. It provides them with technical training, professional certifications, and mentoring services, with the aim of expanding their professional network and expanding the role of women and the LGBTQI+ community in information technology and cybersecurity.[286] The project builds upon the Switch Sea initiative, funded, and implemented by Australia and described below.

- Association of Southeast Asian Nations (ASEAN):
    - **ASEAN Cyber Capacity Program (ACCP):** The program, established in 2016 by Singapore, aims to build cyber capacity in ASEAN members.[287] Upon its establishment in 2016, Singapore allocated over USD 7 million funding for an initial five years. ACCP has since been renewed. The program targets a wide audience, ranging from diplomats to technical operators and analysts. The ACCP

[283] www.laocert.gov.la/activity/10
[284] www.asiapacific.unwomen.org/en/digital-library/publications/2023/05/advancing-the-women-peace-and-security-agenda-and-inclusive-governance
[285] www.thegfce.org/women-in-international-security-and-cyberspace-fellowship/
[286] www.cybilportal.org/projects/switch-supporting-women-in-technical-and-research-project/
[287] www.csa.gov.sg/docs/default-source/csa/documents/sicw-2016/factsheet_accp_final.pdf?sfvrsn=a45aecbb_0#:~:text=Cyber%20Capacity%20Programme-,The%20ASEAN%20Cyber%20Capacity%20Programme%20(ACCP)%20aims%20to%20build%20cyber,secure%20and%20resilient%20ASEAN%20cyberspace.

includes a series of workshops and seminars, as well as the ASEAN Ministerial Conference on Cybersecurity.[288]

- **ASEAN-Singapore Cybersecurity Centre for Excellence (ASCCE):** ASCCE is linked to the ACCP. It extends the scope of the program to include trainings on cyber-legislation development, information sharing among Computer Emergency Response Teams (CERTS), and cooperation with non-ASEAN members, including Korea, Australia, the US, and the UK, in designing cyber capacity-building programs.[289]

- **ASCCE-UK Digital Diplomacy Course:** The Singapore Cybersecurity Agency and the UK Foreign, Commonwealth and Development Office jointly funded and implemented the course in September 2022. The project sought to educate ASEAN policy makers on cybersecurity and digital security matters.[290]

- **Third Country Training Program:** The Singaporean Ministry of Foreign Affairs and the United States Department of State have been running cybersecurity workshops for ASEAN members since 2016. The program, implemented by the US Department of Homeland Security, consists of a yearly workshop where ASEAN member states share best practices on cybersecurity development.[291]

- **ASEAN Cyber Capacity Development Project**: The Japan-ASEAN integration Fund funded the project, while Interpol implemented it. The project, which ran from January 2016 to December 2021, focused on building the capabilities of ASEAN member states to fight cybercrime.[292]

- Australia
  - **International Law in the Cyber Era**: Cyber Law International delivered the programme with the financial support of DFAT from May 2020 to July 2021. The project focused on the links between human rights and cybersecurity, including the management of harmful content online and online surveillance, as well as the risks associated with the E-provision of public services.[293]

  - **Strengthening Digital Media Literacy in the Mekong:** DFAT funded the project, which was delivered by the International Foundation for Electoral Systems. The programme targeted women, minorities, and vulnerable communities, with the aim of strengthening their digital media literacy, and their ability to recognise and counter harmful content online.[294]

[288] www.cybilportal.org/projects/asean-cyber-capacity-programme-accp/
[289] www.cybilportal.org/projects/asean-singapore-cybersecurity-centre-for-excellence-ascce/
[290] www.cybilportal.org/projects/ascce-uk-digital-diplomacy-course/
[291] www.cybilportal.org/projects/singapore-united-states-third-country-training-programme-tctp-cybersecurity-workshops/
[292] www.cybilportal.org/projects/asean-cyber-capacity-development-project/
[293] www.cybilportal.org/projects/international-law-in-the-cyber-era-finding-balance-between-state-interests-and-individual-rights-asia-pacific/
[294] www.ifes.org/programs-initiatives/strengthening-digital-media-literacy-mekong-region ; www.cybilportal.org/projects/strengthening-digital-media-literacy-in-the-mekong/

- **Multi-phase Cybersecurity Program to Critical Infrastructure Organisations**: The Australian Cyber and Critical Tech Cooperation Program funded this initiative, while Retrospect Lab delivered the program in two phases. The first phase aimed to familiarise participants from critical infrastructure organisations with key incident response concepts and a foundational knowledge of cybersecurity. Phase two focused on the deployment of these mechanisms to counter cyberthreats and cybercrime.[295]

- **Defensive Readiness and Cybersecurity Exercise:** The Australian Embassy funded and conducted a training programme for employees of the Lao Department of Cybersecurity. The training sought to provide critical infrastructure organizations with the necessary cybersecurity knowledge to respond to cyber incidents.[296]

- United States:
  - **USAID Digital Asia Accelerator (DAA):**
    - USAID, Development Alternatives Incorporated (DAI) and the US Department of State launched the project in September 2019, with the aim of improving digital skills across Southeast Asia, among other objectives.
    - DAA includes the Cyber for Her: Upskilling and Competition (August 2023) which aims to attract and empower women to pursue and advance careers in the field of Cybersecurity, and the Women's Digital Inclusion Challenge, which is set to digitally upskill women entrepreneurs and women-led businesses in cybersecurity, and digital economy matters.[297]
    - In 2022, the DAA also launched the Developing Cybersecurity Reporting Expertise for Female Journalists in Asia and the Pacific Program which focused on the importance of the media in promoting digital safety.[298]

  - **The Cyber Capabilities and Capacity Development Project (C3DP):** a two-year project funded by the Bureau of International Narcotics and Law Enforcement Affairs and implemented by Interpol. It aims to develop the capabilities of law enforcement agencies in Southeast Asia to combat cyber-crime. The project also establishes Regional Expert Groups to facilitate knowledge exchanges.[299]

- Vietnam:
  - **Laotian-Vietnamese cooperation on cybersecurity:** the two governments have agreed to cooperate on matters of cybersecurity and E-governance, among other topics. This builds on prior cooperation between the two countries.[300]

- ICT4Peace Foundation:

[295] www.retrospectlabs.com/post/delivering-our-multi-phase-cyber-security-program-in-laos
[296] www.laotiantimes.com/2023/02/24/australian-embassy-trains-lao-it-workers-on-cyber-security/
[297] www.usaid.gov/sites/default/files/2023-05/Digital%20Asia%20Accelerator%20Factsheet_1.pdf
[298] https://www.linkedin.com/posts/asia-pacific-institute-for-broadcasting-development_happy-international-womens-day-2023-theme-activity-7039077437573406720-w8Ov/?originalSubdomain=lk
[299] www.cybilportal.org/projects/cyber-capabilities-and-capacity-development-project-c3dp/
[300] www.xinhuanet.com/english/2019-03/13/c_137891440.htm

- Between 2014 and 2018, ICT4Peace ran an international cybersecurity capacity building program that targeted Laos, among other countries. The program dealt with a wide range of cybersecurity-related topics, including international cooperation in cybersecurity matters, national cybersecurity strategy building, and the establishment of CERTS.[301]

Women in Cybersecurity

- Research indicates that Laos is dependent on international organisations and foreign partners for all its female-focused initiatives. These are mostly focused on the public sector, which underscores the gap in access to cybersecurity education for young girls.

- However, as mentioned above, it is important to highlight the limited available external information regarding projects undertaken by Laotian universities.

[301] www.ict4peace.org/wp-content/uploads/2018/09/Outline-Capacity-Building-20180827.pdf

Mongolia

- The 2020 Global Cybersecurity Index, ranked Mongolia 119th globally and 22nd regionally, with an overall score of 26.34/100.[302] With an internet penetration rate of 84.3 per cent in 2023, the country remains vulnerable to cyber threats.[303]

- Research indicates that Mongolian universities have several cybersecurity-focused programs, as well as computer science and information technology degrees that include cybersecurity modules. The list below includes some examples of these, but is not a comprehensive list of all relevant curricula and universities. However, none of the institutions referenced in this study provide statistics on their student body or advertised women-focused initiatives pertaining to cybersecurity, underscoring a potential lack of opportunities for Mongolian women in cybersecurity.

- At a public and executive level, the government is expected to ramp up cyber capabilities development in light of its Vision 2050 policy, which embraces E-governance and cybersecurity as key elements.[304] However, the country remains reliant on international organisations and foreign partners for public awareness and gender-sensitive initiatives.

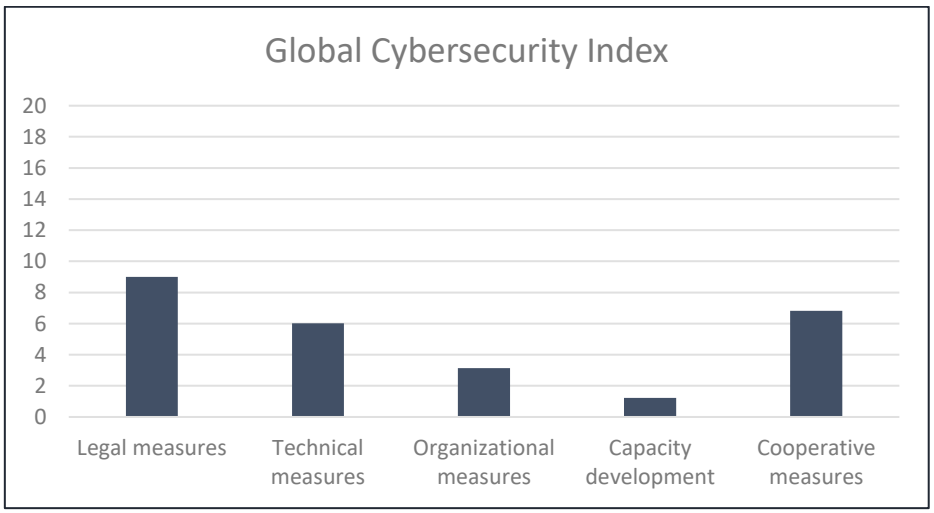


Figure 4: Global Cybersecurity Index score breakdown for Mongolia (ITU, 2020).

Existing Initiatives

Primary and Secondary School

[302] www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
[303] www.datareportal.com/reports/digital-2023-mongolia#:~:text=Mongolia's%20internet%20penetration%20rate%20stood,percent)%20between%202022%20and%202023.
[304] www.vision2050.gov.mn/eng/index.html

- On 22 August 2023, the Ministry of Electronic Development and Communications launched a special class on cybersecurity for 10th graders at the Shutis General Education High School.[305]

Higher Education and Research

- The National Defence University (MNDU) offers a bachelor's degree in military communications engineering and a master's degree in systems security, both of which cover cybersecurity modules.[306]

- MNDU also hosts the Cybersecurity Training Centre. The Centre, run in cooperation with the Indian government, focuses on cyber defence research and facilitates bilateral knowledge exchanges between the two countries.[307]

- The Mongolian University of Science and Technology offers bachelor's and master's degrees in information networks and security. The Department of Information Networks and Security also accepts PhD candidates.[308] It also runs exchange programs with Soon Chun Hyang University in Korea and the Information and Communication Technology Department of the University of Moscow.

- Mongolian National University offers bachelor's, masters and doctoral degrees in information technology and computer science, all of which cover cybersecurity modules.[309] The head of the Department and several faculty members are women.[310]

- Ider University offers a bachelor's degree in information technology, which covers cybersecurity modules.[311]

Professional Training and Certification

Universities and Education Institutions:

- The Information Communication Technology Training Centre at the Mongolian University of Science and Technology offers CISCO certified courses such as, Cisco Certified Network Associate (CCNA) and Cisco Certified Network Professional (CCNP), as well as Microsoft certified courses such as, Microsoft Certified Solution Associate (MCSA).[312]

Private and International Providers:

- Research indicates that private entities are the most common providers of cybersecurity training and certification in Mongolia. These usually have location-specific websites for each country they operate in but offer the same curricula and programmes.

[305] www.mddc.gov.mn/eng/14270/
[306] http://mndu.gov.mn/bhis1/mn/%d0%bd%d2%af%d2%af%d1%80/
[307] www.newindianexpress.com/world/2022/sep/06/rajnathinaugurates-cyber-security-training-centre-in-mongolia-discusses-defence-relations-2495483.html
[308] www.sict.edu.mn/en/257/196
[309] www.seas.num.edu.mn/dep/ics/training/bachelor
[310] www.seas.num.edu.mn/dep/ics/aboutus/teachers
[311] www.ider.edu.mn/copy-3-of-монгол-хэл-уран-зохиолын-багш-6
[312] www.sict.edu.mn/en/257/196

- The Knowledge Academy offers certified cybersecurity professional trainings.[313]
- Mildain offers a range of cybersecurity courses, including CISCO training, ethical hacking, and risk and information systems control.[314]
- Unichrone offers certified information system security professional training.[315]
- SpocLearn offers certified ethical hacker training.[316]

Public and Executive Awareness

National initiatives:

- E-Mongolia Academy: the academy, established in January 2022 as a state-owned enterprise, has a department for information security which runs training for civil servants on information security.[317]
- Mongolian Cyber Police: the police routinely publishes cybersecurity and online safety articles and tips.[318]

Regional and international initiatives:

- United Nations:
    - **Regional Framework towards Peaceful, Inclusive Societies:** The UN Women Regional Office for Asia and the Pacific developed the framework with the aim of including women in sustainable governance and peace-building processes, while allowing them to benefit from sustained peace and gender-responsive laws. The framework includes provisions for an increased presence of women in emerging areas, including cybersecurity.[319]
    - **Women in International Security and Cyberspace Fellowship:** The United National Institute for Training and Research established the fellowship in 2019, with funding coming from Australia, the United States, the United Kingdom, Canada, the Netherlands, and New Zealand. The Fellowship aims to train female diplomats from numerous regions, including East Asia, who participate at the United National cyber negotiations. The project seeks to upskill them in cyber governance matters, while ensuring equal and effective representation at the negotiation table.[320]
- World Bank:

[313] www.theknowledgeacademy.com/mn/courses/cyber-security-training/certified-cyber-security-professional-ccs-pro-/
[314] www.mildaintrainings.com/loc/cyber-security-training-in-mongolia/
[315] www.unichrone.com/mn/cissp-certification-training
[316] www.spoclearn.com/mn/courses/cybersecurity/
[317] www.ema.gov.mn/eng/p1 ; https://mddc.gov.mn/eng/14227/
[318] www.cyber.police.gov.mn/
[319] www.asiapacific.unwomen.org/en/digital-library/publications/2023/05/advancing-the-women-peace-and-security-agenda-and-inclusive-governance
[320] www.thegfce.org/women-in-international-security-and-cyberspace-fellowship/

- **Smart Government II Project:** the project aims to strengthen cybersecurity capabilities in the Mongolian public sector, among other objectives. The final aim is to aid the development of the country's digital economy.[321]

- OECD:
  - **Confidence-Building Measure Customised Implementation Support:** the project, which finished in December 2021, aimed to promote global cyber stability between states, including Mongolia. To do so, the OECD supported national cybersecurity capacity building.[322]
- NATO:
  - **Science for Peace and Security Program:** between 2017 and 2020, NATO supported cyber defence capacity building in Mongolia. The project included the establishment of a Cyber Incident Response Capability Centre at the Mongolian Ministry of Defence, as well as a Cybersecurity Centre at the General Staff. The latter aims to train Mongolian troops in cyber defence matters. The MoD also received technical support from NATO's Communication and Information Agency.[323]

- United States:
  - **USAID Digital Asia Accelerator (DAA):**
    - USAID, Development Alternatives Incorporated (DAI) and the US Department of State launched the project in September 2019, with the aim of improving digital skills across Southeast Asia, among other objectives.
    - DAA includes the Cyber for Her: Upskilling and Competition (August 2023) which aims to attract and empower women to pursue and advance careers in the field of Cybersecurity, and the Women's Digital Inclusion Challenge, which is set to digitally upskill women entrepreneurs and women-led businesses in cybersecurity, and digital economy matters.[324]
    - In 2022, the DAA also launched the Developing Cybersecurity Reporting Expertise for Female Journalists in Asia and the Pacific Program which focused on the importance of the media in promoting digital safety.[325]

- Japan:
  - **Countermeasures against cybercrime**: a Tokyo-funded initiative which ended in December 2015, and implemented by the Japan International Cooperation Agency. The Agency provided Mongolian police forces and other legal bodies with training on the Japanese experience with cybercrime and the measures the country has put in place to reduce and combat it.[326]

---

[321] www.news.mn/en/797558/
[322] www.cybilportal.org/projects/confidence-building-measure-customized-implementation-support/
[323] www.dnn.mn/н-энхболд-зэвсэгт-хүчинд-кибер-аюулгүй-байдлын-тусгай-хүчний-цэрэг-нэмэгдлээ/ ; https://www.army-technology.com/news/nato-completes-project-to-enhance-mongolias-cyber-defence-capability/
[324] www.usaid.gov/sites/default/files/2023-05/Digital%20Asia%20Accelerator%20Factsheet_1.pdf
[325] https://www.linkedin.com/posts/asia-pacific-institute-for-broadcasting-development_happy-international-womens-day-2023-theme-activity-7039077437573406720-w8Ov/?originalSubdomain=lk
[326] www.cybilportal.org/projects/countermeasures-against-cybercrime/

- **Project for Development of Human Resources in Cybersecurity and Related Advanced ICT:** Tokyo ICT and the JICA implemented the project alongside the Ministry of Digital Development. The program focused on cybersecurity training for university professors and helping Mongolian institutions develop cybersecurity curricula.[327]

Women in Cybersecurity

- Research indicates that Mongolian institutions do not tend to engage in gender-based cybersecurity capability development programs. Some of the universities mentioned in this chapter have female-led faculties, though women seem to remain a minority in the sector. In regard to public and executive awareness, Vision 2050 includes several provisions to enhance gender equality in the country, but none of these relate to information technologies and cybersecurity. As such, international organisations are still leading the way in terms of women-focused initiatives.

[327] www.tokyo-ict.com/en/international-cooperation/activities-in-mongolia/

Thailand

- The 2020 Global Cybersecurity Index ranked Thailand 43rd globally and 9th regionally with an overall score of 86.5/100.[328] It is the second highest-ranking country in this cohort after Indonesia.

- Research indicates that several Thai universities offer cybersecurity degrees, as well as computer science and information technology degrees that cover cybersecurity modules. The list below includes some examples of these, but is not a comprehensive list of all relevant curricula and universities. The government is also very active in nurturing a cyber-aware culture, with initiatives such as the Thailand National Week, the Cyber Defence Day Conference, and the Thailand Cybersecurity Awards.[329] Thai students also routinely participate in the Cyber SEA games.[330]

- The government has also taken steps to promote female participation in the sector, though research indicates that women make up only 5 per cent of cybersecurity practitioners.[331]

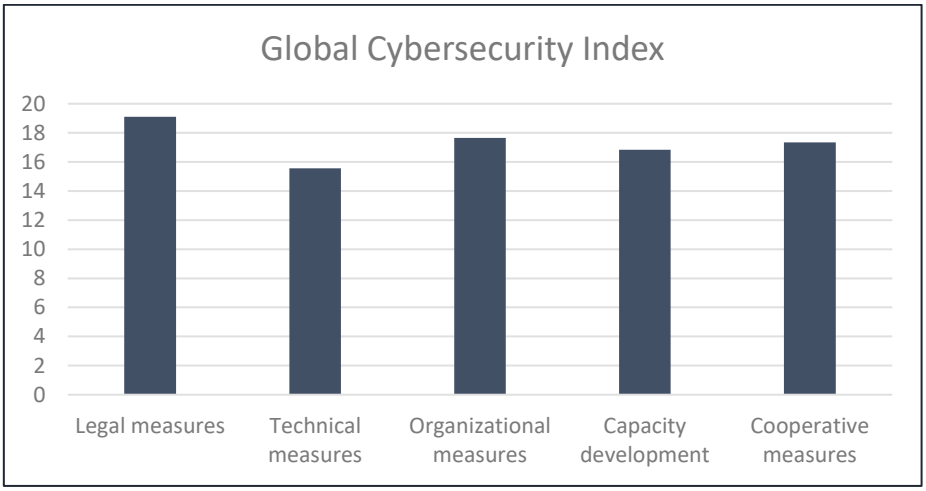


Figure 5: Global Cybersecurity Index score breakdown for Thailand (ITU, 2020).

Existing Initiatives

Higher Education and Research

- Chulachomklao Royal Military Academy offers a bachelor's degree in cybersecurity.[332]

- Bangkok University offers a bachelor's degree in computer science with a focus on data science and cybersecurity.[333]

[328] www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
[329] www.huawei.com/en/news/2022/8/thailand-prime-minister-award ; www.thncw.com/ ; www.cdicconference.com/
[330] www.ctf.in.th/tag/cyber-sea-game-2022/
[331] www.news.microsoft.com/th-th/2022/04/19/women-cybersecurity-en/
[332] www.academic.crma.ac.th/cyber-security.html
[333] www.bu.ac.th/th/it-innovation/datascience-cybersecurity

- Mahidol University offers a master's degree in cybersecurity and Information Assurance. Reports indicate that half of the faculty is female.[334] The University also offers a PhD in Computer Science that covers cybersecurity.[335]

- Chiang Mai University offers bachelor's degrees in computer engineering, information systems, and network engineering. It also offers a master's degree in data science and a doctoral degree in computer science, both of which incorporate cybersecurity modules.[336]

- The Asian Institute of Technology offers master's and doctoral degrees in computer science that cover aspects of cybersecurity.[337]

- King Mongkut's Institute of Technology Ladkrabang offers bachelor's and master's degrees in information technology that cover cybersecurity subjects.[338]

- Kohn Kaen University offers bachelor's and master's degrees in computer engineering that incorporate cyber courses.[339]

- The South Korean Government established ASEAN Cyber University in 2009 and has been funding it ever since. Seoul University implements the initiative, which includes the opening of E-learning centres in Cambodia, Laos, Thailand, Myanmar, and Vietnam.[340]

Professional Training and Certification

Universities and Education Institutions:

- The Asian Institute of Technology offers a professional development training programme called 'Safeguarding Organizations: Implementing Effective Measures Through Cybersecurity for businesses.'[341] On 25 September 2023, it will also run an initiative titled 'Capacity Development and Training for Cyber Insurance Specialists'.[342]

Private and International Providers:

- Research indicates that private entities are the most common providers of cybersecurity training and certification in Thailand. These usually have location-specific websites for each country they operate in, but offer the same curricula and programmes.

- ISACA Thailand Chapter offers a Certification for Information Security Managers. The certification focuses on information security governance, information security risk management, and information security program and incident management.[343] ISACA

[334] www.ict.mahidol.ac.th/our-programs/master-of-science-in-cyber-security-and-information-assurance/
[335] www.ict.mahidol.ac.th/our-programs/doctor-of-philosophy-in-computer-science/
[336] www.cmu.ac.th/en/Faculty/course_detail/77906e06-b686-454f-80e0-84e1521ab196 ; www.cmu.ac.th/en/Faculty/course_detail/f59f564f-ea8c-4df6-8fe1-7d915b13531b ; www.cmu.ac.th/en/Faculty/course_detail/531f509d-e7fb-4e8c-8a2d-4a2e1563c5cb ; www.cmu.ac.th/en/Faculty/course_detail/a3bcbd87-d8e3-42cb-9d3e-39e75b577c7b
[337] www.ait.ac.th/program/computer-science/
[338] www.it.kmitl.ac.th/th/program/it-program/it-subjects/
[339] www.en.kku.ac.th/web/en/undergraduate/
[340] www.universityworldnews.com/post.php?story=20110610213112 66 ; www.aseanoer.net/
[341] www.ait.ac.th/event/safeguarding-organizations-implementing-effective-measures-through-cybersecurity/
[342] www.ait.ac.th/event/capacity-development-and-training-for-cyber-insurance-specialist/
[343] www.isaca.org/credentialing/cism

also offers other certifications including training for information systems auditing, risk and information systems control, and data privacy solutions engineering and governance of enterprise IT. [344]

- NobleProg offers courses such as, Cipher Trust Manager, Cybersecurity with Python, CCTV Security, Security Management, Cloudflare Essentials, Honeywell Security System, Cybersecurity Awareness Training, Open Authentication, Synk and OpenStack Security.[345]

- The Knowledge Academy offers certified cybersecurity professional training (CCS-PRO). Other offering cover areas such as Incident Response, Cyber awareness, and Cyber Security Risk Management.[346]

- Mildain the website offers a range of cybersecurity courses, including CISCO training, ethical hacking, and risk and information systems control.[347]

- SkillLogic offers a cybersecurity certification course.[348]

Public and Executive Awareness

National initiatives:

- The National Cybersecurity Agency (NSCA) provides cybersecurity capacity development to practitioners in seven critical infrastructure areas: national security, public service, banking and finance, information technology and telecoms, transport and logistics, energy, and public utilities, and public health.[349]

- The National Broadcasting and Telecommunications Commission (NBTC) of Thailand offers an initiative titled 'Human Capacity Building in Cybersecurity and critical infrastructure protection.' The NBTC cooperated with the International Telecommunication Union for the implementation of this programme which ended in December 2016. The aim of the project was to upskill government agencies and critical infrastructure practitioners in cybersecurity.[350]

- The NCSA hosts a Women Thailand Cyber Top Talent competition. Since 2022, NCSA has been organising the competition, with the aim of increasing female participation and recognition in cyber. The program is run in collaboration with Huawei technologies.[351]

Regional and international initiatives:

---

[344] www.isaca-bangkok.org/
[345] www.nobleprog.co.th/cybersecurity-training
[346] www.theknowledgeacademy.com/th/courses/cyber-security-training/
[347] www.mildaintrainings.com/loc/cyber-security-training-in-thailand-th/
[348] https://skillogic.com/cyber-security-certification-course-thailand/
[349] https://opengovasia.com/thailand-proposes-additional-regulations-to-boost-cybersecurity/
[350] https://cybilportal.org/projects/human-capacity-building-in-cybersecurity-and-critical-infrastructure-protection/
[351] https://ctf.in.th/womenctf2022/

- United Nations:
    - **Regional Framework towards Peaceful, Inclusive Societies:** The UN Women Regional Office for Asia and the Pacific developed the framework with the aim of including women in sustainable governance and peace-building processes, while allowing them to benefit from sustained peace and gender-responsive laws. The framework includes provisions for the increased presence of women in emerging areas, including cybersecurity.[352]

    - **Women in International Security and Cyberspace Fellowship:** The United National Institute for Training and Research established the fellowship in 2019, with funding from the governments of Australia, the United States, the United Kingdom, Canada, the Netherlands, and New Zealand. The Fellowship aims to train female diplomats from numerous regions, including East Asia, who participate at the United National cyber negotiations. The project seeks to upskill them in cyber governance matters, while ensuring equal and effective representation at the negotiations table.[353]

- Asia Pacific Internet Development Fund (APIDIT):
    - **Supporting Women in Technical and Research Project (Switch):** APIDIT and the Asia Pacific Network Information Centre kickstarted Switch in June 2022. The project seeks to support the career development of women, and LGBTQI+ individuals working on internet development. It provides them with technical training, professional certifications, and mentoring services, with the aim of expanding their professional network and expanding the role of women and the LGBTQI+ community in information technology and cybersecurity.[354] The project builds upon the Switch Sea initiative, which is funded and implemented by the Australian government.

- Australia:
    - **Supporting Women in Internet Research Leaders in Southeast Asia (Switch Sea):** DFAT implemented the project from May 2020 to December 2021 with the aim of fostering diversity and gender empowerment within the internet industry in Southeast Asia. The project started with a cohort of 100 women and LGBTQI+ engineers, providing them with education, training and mentoring in both technical and leadership matters.[355]

    - **Strengthening Digital Media Literacy in the Mekong:** DFAT funded and implemented by the International Foundation for Electoral Systems. The program targeted women, minorities, and vulnerable populations with the aim of

[352] www.asiapacific.unwomen.org/en/digital-library/publications/2023/05/advancing-the-women-peace-and-security-agenda-and-inclusive-governance
[353] www.thegfce.org/women-in-international-security-and-cyberspace-fellowship/
[354] www.cybilportal.org/projects/switch-supporting-women-in-technical-and-research-project/
[355] www.cybilportal.org/projects/switch-sea-fostering-womens-technical-leadership-in-the-internet-industry-in-southeast-asia/

strengthening their digital media literacy and their ability to recognise and counter harmful content online.[356]

- **Multi-phase cybersecurity programme for critical infrastructure organisations:** The Australian Cyber and Critical Tech Cooperation Program funded the initiative. Retrospect Lab delivered the program in two phases. The first phase aimed to familiarise participants from critical infrastructure organisations with key incident response concepts and the foundational knowledge of cybersecurity. Phase two focused on the deployment of these mechanisms to counter cyberthreats and cybercrime.[357]

  Cyber Bootcamp Project: Between 22 and 26 February 2021, Australia delivered a digital bootcamp to Thai officials on cyber challenges and cyber resilience.[358]

- Association of Southeast Asian Nations (ASEAN):
  - **ASEAN Cyber Capacity Program (ACCP):** the programme, established in 2016 by the Singaporean government, aims to build cyber capacity in ASEAN member countries.[359] Upon its establishment in 2016, Singapore allocated over USD 7 million funding for an initial five years. The ACCP has since been renewed. The program targets a wide audience, ranging from diplomats to technical operators and analysts. The ACCP includes a series of workshops and seminars, as well as the ASEAN Ministerial Conference on Cybersecurity.[360]

  - **ASEAN-Singapore Cybersecurity Centre for Excellence (ASCCE):** the ASCCE is linked to the ACCP. It extends the scope of the program to include training on cyber-legislation development, information sharing among Computer Emergency Response Teams (CERTS), and cooperation with non-ASEAN members, including Korea, Australia, the United States, and the United Kingdom, in designing cyber capacity-building programs.[361]

  - **ASCCE-UK Digital Diplomacy Course:** the Singapore Cybersecurity Agency and the UK Foreign, Commonwealth and Development Office jointly funded and implemented the course in September 2022. The project sought to educate ASEAN policy makers on cybersecurity and digital security matters.[362]

[356] www.ifes.org/programs-initiatives/strengthening-digital-media-literacy-mekong-region ; www.cybilportal.org/projects/strengthening-digital-media-literacy-in-the-mekong/
[357] www.retrospectlabs.com/post/delivering-our-cctcp-in-thailand
[358] www.internationalcybertech.gov.au/Cyber-Bootcamp-Project
[359] www.csa.gov.sg/docs/default-source/csa/documents/sicw-2016/factsheet_accp_final.pdf?sfvrsn=a45aecbb_0#:~:text=Cyber%20Capacity%20Programme-,The%20ASEAN%20Cyber%20Capacity%20Programme%20(ACCP)%20aims%20to%20build%20cyber,secure%20and%20resilient%20ASEAN%20cyberspace.
[360] www.cybilportal.org/projects/asean-cyber-capacity-programme-accp/
[361] www.cybilportal.org/projects/asean-singapore-cybersecurity-centre-for-excellence-ascce/
[362] www.cybilportal.org/projects/ascce-uk-digital-diplomacy-course/

- **Third Country Training Program:** The Singaporean Ministry of Foreign Affairs and the United States Department of State have been running cybersecurity workshops for ASEAN members since 2016. The program, implemented by the US Department of Homeland Security, consists of a yearly workshop where ASEAN member states share best practices on cybersecurity development.[363]

- **ASEAN Cyber Capacity Development Project:** the Japan-ASEAN integration Fund funded the project, while Interpol implemented it. The project, which ran from January 2016 to December 2021, focused on building the capabilities of ASEAN member states to fight cybercrime.[364]

- **Building Anti-Cybercrime Capacity in ASEAN Through Simulation Exercises:** Canada funded the project, which ended in March 2023. The initiative set up bilateral simulation exercises, as well as a regional one, with the aim of testing cyber incident preparedness.[365]

- United States:
  - **USAID Digital Asia Accelerator (DAA):**
    - USAID, Development Alternatives Incorporated (DAI) and the US Department of State launched the project in September 2019, with the aim of improving digital skills across Southeast Asia, among other objectives.
    - DAA includes the Cyber for Her: Upskilling and Competition (August 2023) which aims to attract and empower women to pursue and advance careers in the field of Cybersecurity, and the Women's Digital Inclusion Challenge, which is set to digitally upskill women entrepreneurs and women-led businesses in cybersecurity, and digital economy matters.[366]
    - In 2022, the DAA also launched the Developing Cybersecurity Reporting Expertise for Female Journalists in Asia and the Pacific Program which focused on the importance of the media in promoting digital safety.[367]

  - **The Cyber Capabilities and Capacity Development Project (C3DP):** a two-year project funded by the Bureau of International Narcotics and Law Enforcement Affairs and implemented by Interpol. It aims to develop the capabilities of law enforcement agencies in Southeast Asia to combat cyber-crime. The project also establishes Regional Expert Groups to facilitate knowledge exchanges.[368]

[363] www.cybilportal.org/projects/singapore-united-states-third-country-training-programme-tctp-cybersecurity-workshops/
[364] www.cybilportal.org/projects/asean-cyber-capacity-development-project/
[365] www.cybilportal.org/projects/building-anti-cybercrime-capacity-in-asean-through-simulation-exercises/
[366] www.usaid.gov/sites/default/files/2023-05/Digital%20Asia%20Accelerator%20Factsheet_1.pdf
[367] https://www.linkedin.com/posts/asia-pacific-institute-for-broadcasting-development_happy-international-womens-day-2023-theme-activity-7039077437573406720-w8Ov/?originalSubdomain=lk
[368] www.cybilportal.org/projects/cyber-capabilities-and-capacity-development-project-c3dp/

- The US cybersecurity and infrastructure agency also ran a **cyber hygiene workshop** with the Indonesian BSSN and the Thai NSCA on 21 April 2023.[369] The workshop focused on covered information technology/operational technology (IT/OT), industrial control systems, threat actors, threat intelligence, cyber-attack frameworks, workforce development tools, and case studies of common attacks.

- Estonia:
  - **Introduction Estonian ICT solutions:** the program, which ran from January 2015 to December 2017, provided Thai officials with 10 training sessions per year on approaches to interoperability and legal frameworks of E-government.[370]

- ICT4Peace Foundation:
  - Between 2014 and 2018, ICT4Peace ran an international cybersecurity capacity building programme that targeted Thailand, among other countries. The initiative dealt with a wide range of cybersecurity-related topics, including international cooperation in cybersecurity matters, national cybersecurity strategy building, and the establishment of CERTS.[371]

- Microsoft:
  - **Enhancing cybersecurity digital skills for 4,000 Thais:** Microsoft provided digital security trainings to 4,000 Thai citizens, targeted at women in particular. The lessons covered the basics of cybersecurity.[372]
  - **Microsoft Women@Cybersecurity:** on 19 April 2022, Microsoft and the NCSA hosted the event with the aim of familiarising women high school and university students with careers in cybersecurity.[373]

Women in Cybersecurity

- Thailand is one of the few countries in this research that offer domestic female-focused initiatives. Nevertheless, international partners and private organisations remain the primary providers of gender-sensitive programmes, especially in the public sector. Overall, Thailand's eagerness to build a cyber-aware culture from an early age, via competitions and simulations, suggests that the Thai market presents fewer gaps in its capacity-building strategy than its peers included in this study.

[369] https://www.cisa.gov/news-events/news/cisa-building-cyber-hygiene-capacity-thailand-philippines-and-indonesia
[370] https://cybilportal.org/projects/introducing-estonian-ict-solutions-to-delegations-from-developing-countries/
[371] www.ict4peace.org/wp-content/uploads/2018/09/Outline-Capacity-Building-20180827.pdf
[372] https://news.microsoft.com/th-th/2022/10/28/global-skills-initiative-gsi2-en/
[373] https://news.microsoft.com/th-th/2022/04/19/women-cybersecurity-en/

Conclusion

- Educational institutions, law enforcement agencies and international partners make up most of the cybersecurity capacity development market in the APAC region. Research found that ASEAN is the most important cybersecurity capability development provider in Southeast Asia.

- Research indicates that all countries in the study have strong educational offerings, with degrees that provide comprehensive training on cybersecurity. While women sit on the faculties of these institutions, none of them provide gender-based initiatives to increase women's access to higher education in the field.

- Research identified significant gaps in female-focused and gender-based initiatives in the public sector in all countries. International organisations are the key providers of these, though the programmes often target specific demographics - either civil servants or MSMEs – leaving significant gaps in the market.

- Private sector entities do not engage in any specific female-focused initiatives, thus increasing barriers of access to vocational training and professional certifications.

Chapter 5: Gap Assessment

Introduction

This chapter combines the findings from the future workforce assessment (demand-side of cybersecurity workforce ecosystem) and the market assessment (supply-side of cybersecurity workforce ecosystem) to produce an assessment to understand the gap between the anticipated skill requirements and current skills and training capability and capacity across the five research focus countries.

Methodology

The gap assessment was completed by firstly isolating the overlapping Technical Cybersecurity Job Roles and additional Cyber Security Workforce Requirements identified in the Future Workforce Assessment. This resulted in 5 priority technical cybersecurity job roles being identified as a starting point for cybersecurity skills development and training.

Secondly, the range of existing education and training offerings and capabilities identified in the Market Assessment were mapped against each of the five priority Technical Cybersecurity Job Roles and the additional cyber security workforce requirements.

Lastly, a gap assessment was completed for each of the five priority Technical Cybersecurity Job Roles and additional Cyber Security Workforce Requirement areas to determine the extent to which cybersecurity education and training provisions and capabilities existed across the five research focus countries. This process illustrated in Figure 4.

Figure 4 - Gap Assessment Process

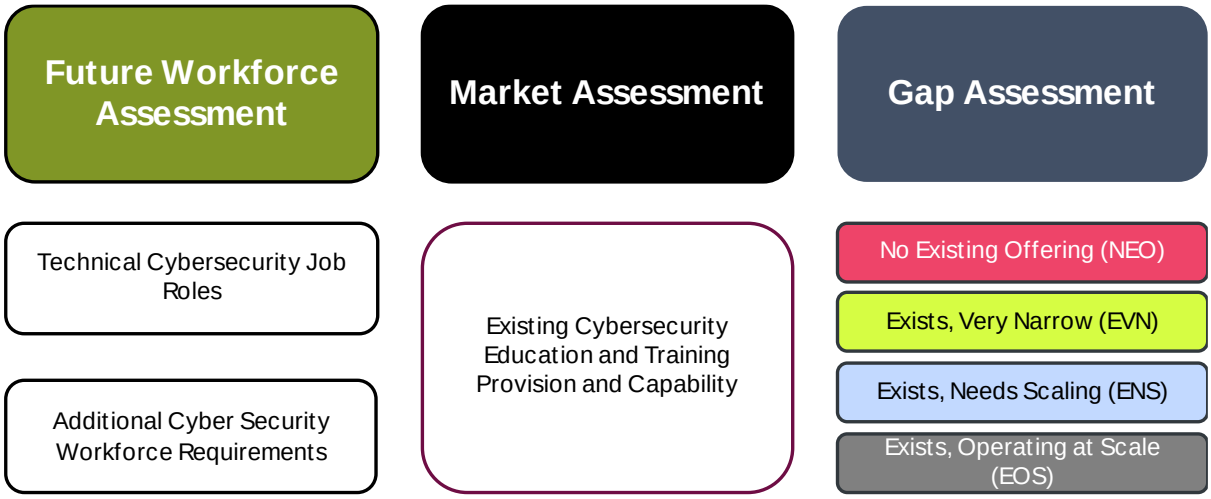


Table 1 details the rating system used in the gap assessment.

Table 4 - Gap Assessment Rating Criteria

Gap Assessment Rating	Description
No Existing Offering (NEO)	The market assessment was unable to identify any existing cybersecurity education and training provisions or capabilities to support skills development in this area.
Exists, Very Narrow (EVN)	The market assessment identified existing cybersecurity education and training provisions or capabilities to support skills development in this area. However, such offerings and capabilities are very narrow and would unlikely be sufficient to support the expected future workforce and skills requirement.
Exists, Needs Scaling and External Validation (ENS)	The market assessment identified existing cybersecurity education and training provisions or capabilities to support skills development in this area. Such offerings and capabilities are suitable to support expected future workforce and skills requirement, however, increase scale and independent external validation is required to support future demand and interoperability.
Exists, Operating at Scale (EOS)	The market assessment identified existing cybersecurity education and training provisions or capabilities to support skills development in this area. Such offerings and capabilities are suitable, and externally validated to support expected future workforce and skills requirement and additional education and training provisions are not required.

Gap Assessment Findings

Cambodia

The gap assessment for Cambodia completed below found that for the priority Technical Cybersecurity Job Roles included the assessment that cybersecurity education and training provision existed across all roles:

- For the three roles Cyber Incident Responder, Cyber Legal, Policy and Compliance Officer, and Cyber Threat Intelligence Specialist, the gap was assessed as 'Exists, Very Narrow'
- For the two roles Cybersecurity Risk Manager and Penetration Tester, the gap was assessed as 'Exists, Needs Scaling and External Validation'.

The market assessment identified existing cybersecurity education and training provisions or capabilities to support skills development in this area. Such offerings and capabilities are suitable to support expected future workforce and skills requirement, however, increase scale and independent external validation is required to support future demand and interoperability.

When it comes to additional cybersecurity workforce requirements which covers education and training for Senior Executives, Managers, IT Staff and the General Workforce, the gap was more significant. A formal review of such offerings is therefore recommended to ensure that all such available offerings have been captured that may have fallen outside the data sources available for this research project.

Technical Cybersecurity Job Role

Role	Market Offering	Gap Assessment Rating
Cyber Incident Responder	**American University of Phnom Penh** • Certificate in cybersecurity **Mildain Training** • Certified Network Defender (CND) Certification Training • Certified Information Security Manager (CISM) Training	EVN
Cyber Legal, Policy and Compliance Officer	**Beltei International University** • Bachelors in Computer Networking and Cybersecurity **American University of Phnom Penh** • Certificate in cybersecurity **Mildain Training** • Certified Information Security Manager (CISM) Training	EVN
Cyber Threat Intelligence Specialist	**CamTech** • Bachelors in Cyber Security **University of Puthisastra** • Masters in IT with major in Cybersecurity **American University of Phnom Penh** • Certificate in cybersecurity **The Knowledge Academy** • Certified cybersecurity professional training (CCS-PRO)	EVN
Cybersecurity Risk Manager	**University of Puthisastra** • Masters in IT with major in Cybersecurity **American University of Phnom Penh** • Certificate in cybersecurity **The Knowledge Academy** • Certified cybersecurity professional training (CCS-PRO) **Mildain Training** • Certified in Risk and Information Systems Control (CRISC) Certification Training • Certified Information Security Manager (CISM) Training	ENS
Penetration Tester	**CamTech** • Bachelors in Cyber Security **Beltei International University** • Bachelors in Computer Networking and Cybersecurity	ENS

	Cambodia Academy of Digital Technology • Professional certification in ethical hacking and information technology **The Knowledge Academy** • Certified cybersecurity professional training (CCS-PRO) **Mildain Training** • Certified Ethical Hacker (CEH v10) Training • Certified Security Analyst (ECSA v10) Training	

Additional Cybersecurity Workforce Requirements

Role	Market Offering	Gap Assessment Rating
Senior Executives	*Not Identified*	NEO
Managers	*Not Identified*	NEO
IT Staff	*Not Identified*	NEO
General Workforce	**The Knowledge Academy** • Certified cybersecurity professional training (CCS-PRO) **Open Development Cambodia** • Awareness Day **Mildain Training** • Awareness Training **Step It Academy** • Cybersecurity Essentials	ENS

Indonesia

The gap assessment for Indonesia completed below found that for the priority Technical Cybersecurity Job Roles included the assessment that cybersecurity education and training provision existed across all roles:

- For all five of the priority roles of Cyber Incident Responder, Cyber Legal, Policy and Compliance Officer, Cyber Threat Intelligence Specialist, Cybersecurity Risk Manager and Penetration Tester, the gap was assessed as 'Exists, Very Narrow'. Such offerings and capabilities would unlikely be sufficient to support the expected future workforce and skills requirement.

The market assessment identified that Indonesia presents a wide array of cyber security capacity building initiatives to support skills development targeting students, civil servants and government officials. These offerings are also supplemented in ASEAN and other regional initiatives. Indonesia can build on this foundation and current offerings and capabilities to further develop and expand education and training pathways that focus on prepare and certify aspiring cybersecurity workers for the priority technical roles required in the country.

The market assessment found that at least two Indonesian institutions have implemented gender-based programs to encourage female participation in the cyber sector at both educational and

professional levels, but the country remains reliant on international organisations and foreign partners for women-facing initiatives.

Similar to the priority technical roles, when it comes to additional cybersecurity workforce requirements covering education and training for Senior Executives and the General Workforce, the gap was assessed as 'Exists, Very Narrow' and such offerings and capabilities would unlikely be sufficient to support the expected future workforce and skills requirement. Furthermore, the gap for Managers and IT Staff was more significant and a formal review of such offerings is recommended to ensure that all such available offerings have been captured that may have fallen outside the data sources available for this research project.

Technical Cybersecurity Job Role

Role	Market Offering	Gap Assessment Rating
Cyber Incident Responder	**Binus University** • Bachelors in Cybersecurity **NobleProg** • Cyber Crisis & Communications Planning **ISACA Indonesia Chapter** • Certified Information Security Manager (CISM) Training	EVN
Cyber Legal, Policy and Compliance Officer	**ISACA Indonesia Chapter** • Certified Information Security Manager (CISM) Training	EVN
Cyber Threat Intelligence Specialist	**Binus University** • Bachelors in Cybersecurity	EVN
Cybersecurity Risk Manager	**ISACA Indonesia Chapter** • Certified in Risk and Information Systems Control (CRISC)	EVN
Penetration Tester	**Binus University** • Bachelors in Cybersecurity **SANS** • SEC560: Enterprise Penetration Testing **NobleProg** • Ethical Hacker • Web security with OWASP Testing Framework **Simplilearn** • Post Graduate in Cybersecurity **OWASP Jakarta** • Training on Penetration Testing	EVN

Additional Cybersecurity Workforce Requirements

Role	Market Offering	Gap Assessment Rating
Senior Executives	**NobleProg** • Executive Cyber Security Awareness	EVN
Managers	*Not Identified*	NEO
IT Staff	*Not Identified*	NEO
General Workforce	**NobleProg** • Cybersecurity Awareness Training	EVN

Laos

The gap assessment for Laos completed below found that cybersecurity education and training provision existed for four of the five priority Technical Cybersecurity Job Roles, but not for Cyber Threat Intelligence Specialists:

- For the four roles of Cyber Incident Responder, Cyber Legal, Policy and Compliance Officer, Cybersecurity Risk Manager and Penetration Tester, the gap was assessed as 'Exists, Very Narrow'. Such offerings and capabilities would unlikely be sufficient to support the expected future workforce and skills requirement.
- No existing market offering was found for Cyber Threat Intelligence Specialists

The market assessment identified existing cybersecurity education and training provisions or capabilities to support skills development for many areas, but Laos is dependent on international organisations and foreign partners, particularly for all its female-focused initiatives. Existing offerings are mostly focused on the public sector which underscores the gap in access to cybersecurity education for young girls.

Laos also appears to mostly rely on regional and international initiatives for public and executive awareness. Although offerings and capabilities are suitable to support expected future workforce and skills requirements, increased scale and independent external validation is required to support future demand and interoperability.

When it comes to additional cybersecurity workforce requirements which covers education and training for Senior Executives, Managers and IT Staff, the gap was more significant, and no existing offerings were found. A formal review of such offerings is therefore recommended to ensure that all such available offerings have been captured that may have fallen outside the data sources available for this research project.

Technical Cybersecurity Job Role

Role	Market Offering	Gap Assessment Rating
Cyber Incident Responder	**Mildain Training** • Certified Network Defender (CND) Certification Training • Certified Information Security Manager (CISM) Training	EVN

Cyber Legal, Policy and Compliance Officer	**Mildain Training** • Certified Information Security Manager (CISM) Training	EVN
Cyber Threat Intelligence Specialist	*Not Identified*	NEO
Cybersecurity Risk Manager	**Mildain Training** • Certified in Risk and Information Systems Control (CRISC) Certification Training • Certified Information Security Manager (CISM) Training	EVN
Penetration Tester	**Mildain Training** • Certified Ethical Hacker (CEH v10) Training • Certified Security Analyst (ECSA v10) Training	EVN

Additional Cybersecurity Workforce Requirements

Role	Market Offering	Gap Assessment Rating
Senior Executives	*Not Identified*	NEO
Managers	*Not Identified*	NEO
IT Staff	*Not Identified*	NEO
General Workforce	**The Knowledge Academy** • Cyber Security Awareness Course – Lao People's Democratic Republic **Mildain Training** • Awareness Training	EVN

Mongolia

The gap assessment for Mongolia found that cybersecurity education and training provision existed for four of the five priority Technical Cybersecurity Job Roles, but not for Cyber Threat Intelligence Specialists:

- For the four roles Cyber Incident Responder, Cyber Legal, Policy and Compliance Officer, Cybersecurity Risk Manager and Penetration Tester, the gap was assessed as 'Exists, Very Narrow'. Such offerings and capabilities would unlikely be sufficient to support the expected future workforce and skills requirement.
- No existing market offering was found for Cyber Threat Intelligence Specialists

The market assessment identified existing cybersecurity education and training provisions or capabilities to support skills development in this area. Such offerings and capabilities are suitable to support expected future workforce and skills requirement, however, increased scale and independent external validation is required to support future demand and interoperability.

The market assessment also found that at a public and executive level, the government is expected to ramp up cyber capabilities development in light of its Vision 2050 policy, but the country remains reliant on international organisations and foreign partners for public awareness and gender-sensitive initiatives.

Although an existing (albeit very narrow) market offering was found for General Workforce, when it comes to additional cybersecurity workforce requirements which covers education and training for Senior Executives, Managers and IT Staff, the gap was more significant, and no existing offerings were found. A formal review of such offerings is therefore recommended to ensure that all such available offerings have been captured that may have fallen outside the data sources available for this research project.

Technical Cybersecurity Job Role

Role	Market Offering	Gap Assessment Rating
Cyber Incident Responder	**Mildain Training** • Certified Network Defender (CND) Certification Training • Certified Information Security Manager (CISM) Training	EVN
Cyber Legal, Policy and Compliance Officer	**Mildain Training** • Certified Information Security Manager (CISM) Training	EVN
Cyber Threat Intelligence Specialist	*Not Identified*	NEO
Cybersecurity Risk Manager	**Mildain Training** • Certified in Risk and Information Systems Control (CRISC) Certification Training • Certified Information Security Manager (CISM) Training	EVN
Penetration Tester	**Mildain Training** • Certified Ethical Hacker (CEH v10) Training • Certified Security Analyst (ECSA v10) Training **Spoclearn** • Certified Ethical Hacker (CEH)	EVN

Additional Cybersecurity Workforce Requirements

Role	Market Offering	Gap Assessment Rating
Senior Executives	*Not Identified*	NEO
Managers	*Not Identified*	NEO
IT Staff	*Not Identified*	NEO
General Workforce	**The Knowledge Academy** • Certified Cyber Security professional (CCS-PRO) - Mongolia **Mildain Training** • Awareness Training	EVN

Thailand

The gap assessment for Thailand found that for the priority Technical Cybersecurity Job Roles included the assessment that cybersecurity education and training provision existed across all roles:

- For the four roles of Cyber Incident Responder, Cyber Legal, Policy and Compliance Officer, Cyber Threat Intelligence Specialist and Penetration Tester, the gap was assessed as 'Exists, Very Narrow'. Existing offerings and capabilities would unlikely be sufficient to support the expected future workforce and skills requirement.
- For the role of Cybersecurity Risk Manager, the gap was assessed as 'Exists, Needs Scaling and External Validation', indicating that existing offerings and capabilities are suitable to support expected future workforce and skills requirement, but an increase scale and independent external validation is required to support future demand and interoperability.

The market assessment found that several Thai universities offer cybersecurity degrees, and the government is also very active in nurturing a cyber-aware culture with a range of national cyber initiatives. The research also found that Thailand offers domestic female-focused initiatives and the country's eagerness to build a cyber-aware culture from an early age via competitions and simulations, suggests the Thai market presents fewer gaps in its capacity-building strategy than the other four countries in this study.

When it comes to additional cybersecurity workforce requirements which covers education and training for Senior Executives, Managers, IT Staff and the General Workforce, the gap was assessed as 'Exists, Very Narrow' which indicates there are existing cybersecurity education and training provisions or capabilities to support skills development in this area. However, such offerings and capabilities are very narrow and would unlikely be sufficient to support the expected future workforce and skills requirement.

Technical Cybersecurity Job Role

Role	Market Offering	Gap Assessment Rating
Cyber Incident Responder	**ISACA Bangkok Chapter** • Certified Information Security Manager (CISM) Training **The Knowledge Academy** • Incident Response Training **Chulachomklao Royal Military Academy** • Bachelor of Cybersecurity	EVN
Cyber Legal, Policy and Compliance Officer	**ISACA Bangkok Chapter** • Certified Information Security Manager (CISM) Training	EVN
Cyber Threat Intelligence Specialist	**The Knowledge Academy** • Certified cybersecurity professional training (CCS-PRO)	EVN
Cybersecurity Risk Manager	**Mahidol University** • Master's degree in cybersecurity and Information Assurance **ISACA Thailand Chapter**	ENS

	• Certified Information Security Manager (CISM) Training **ISACA Bangkok Chapter** • Certified Information Security Manager (CISM) Training • Certified in Risk and Information Systems Control (CRISC) Certification Training **NoblePro** • Security Management Training **The Knowledge Academy** • Certified cybersecurity professional training (CCS-PRO) • Cyber Security Risk Management Course **Mildain Training** • Certified in Risk and Information Systems Control (CRISC) Certification Training • Certified Information Security Manager (CISM) Training	
Penetration Tester	**The Knowledge Academy** • Certified cybersecurity professional training (CCS-PRO)	EVN

Additional Cybersecurity Workforce Requirements

Role	Market Offering	Gap Assessment Rating
Senior Executives	**NobleProg** • Cybersecurity Awareness Training **The Knowledge Academy** • Cybersecurity Awareness Training	EVN
Managers	**NobleProg** • Cybersecurity Awareness Training **The Knowledge Academy** • Cybersecurity Awareness Training	EVN
IT Staff	**NobleProg** • Cybersecurity Awareness Training **The Knowledge Academy** • Cybersecurity Awareness Training **Mildain Training** • Awareness Training	EVN
General Workforce	**Noble Prog**	EVN

	• Cybersecurity Awareness Training **The Knowledge Academy** • Certified Cyber Security professional (CCS-PRO) - Thailand **Mildain Training** • Awareness Training	

Regional View

Table 5 - Gap Assessment Rating Matrix by Country for Priority Technical Cybersecurity Roles

Role	Cambodia	Indonesia	Laos	Mongolia	Thailand
Technical Cybersecurity Roles					
Cyber Incident Responder	EVN	EVN	EVN	EVN	EVN
Cyber Legal, Policy and Compliance Officer	EVN	EVN	EVN	EVN	EVN
Cyber Threat Intelligence Specialist	EVN	EVN	NEO	NEO	EVN
Cybersecurity Risk Manager	ENS	EVN	EVN	EVN	ENS
Penetration Tester	ENS	EVN	EVN	EVN	EVN
Additional Workforce Requirements					
Senior Executives	NEO	EVN	NEO	NEO	EVN
Managers	NEO	NEO	NEO	NEO	EVN
IT Staff	NEO	NEO	NEO	NEO	EVN
General Workforce	ENS	EVN	EVN	EVN	EVN

The research identified that for the five priority technical cyber security roles, the vast majority are supported by existing cybersecurity education and training provisions or capabilities to support skills development in these areas. However, these offerings and capabilities are currently very narrow and would unlikely be sufficient to support the expected future workforce and skills requirement in the region. Although region-wide provision was progressive, the assessment found a lack of cybersecurity education and training provisions for Cyber Threat Intelligence Specialist Training in both Laos and Mongolia.

In terms of additional workforce requirements, with the exception of Thailand, the assessment was unable to identify existing cybersecurity education and training provisions or capabilities to support skills development for Senior Executives, Managers and IT Staff. These are significant gaps as senior staff are needed to be able to develop and embed cybersecurity strategies and policies as part of a cybersecurity culture, supported by managers who can apply organisational policies across their teams. The research also identified that there is a gap in training provisions across the region for IT Staff who perform vital roles for organisations in being able to respond to and investigate cyber incidents.

Conclusion

The gap between expected future priority cybersecurity workforce requirements and existing market education and training provisions and capabilities identified in this chapter provides indicative insights into immediate focus points for developing the necessary cybersecurity education and training capacity and capability across the five research focus countries.

Based on the gap assessment, there is evidence to suggest that whilst a range of cybersecurity education and training provision does already exist across the give research focus countries, that in most cases this is quite limited and requires development and scaling in order to service future workforce requirements.

Key Findings and Recommendations

Summary of Key Findings

This report compiles the research findings from the Women's Participation in Southeast Asia's Cybersecurity Sector project which was completed to understand the cybersecurity workforce in Cambodia, Indonesia, Laos, Mongolia and Thailand, identify gaps in the workforce to equip these five countries with the cybersecurity requirements of the future, and understand women's participation in the sector across these five geographies.

Informed by these research findings, the following chapter outlines the opportunities and challenges for the participation of women in the cybersecurity workforce across the five research focus countries and provides recommendations for future capacity building programs.

Opportunities

Full-Utilisation of the Labour Market

Chapter one identified nine strategic drivers that capture and define the key forces that are likely to drive a need for technical cybersecurity skills in the five research focus countries and Southeast Asia region in the future.

- In order to respond to this diverse range of strategic drivers countries will need to ensure the full utilisation of the labour market, both in terms of workforce size as well as composition, to build the necessary capability and capacity to respond to and mitigate cybersecurity risks and threats and facilitate development ambitions.

- There is a significant opportunity for countries to achieve this goal through rapidly increasing the participation of women into cybersecurity training and education and career pathways and fully utilise national labour market potential.

Wide-Ranging Benefits across Society

Chapter two presented insights on the participation of women in the cybersecurity workforce in the Southeast Asian region and explored topics including the different opportunities that could be explored to close the gap.

- There is an opportunity for countries to gain a tremendous benefit from increasing the participation rate of women in the cybersecurity workforce with the research identifying perceived national and societal benefits including:

    - Improved Solutions: Developing more effective cybersecurity solutions for end users by improving the understanding of women and girls' digital experiences, preferences, and behaviours.

    - Diverse Workforce: The positive impact that a more diverse workforce can have for the efficiency and effectiveness of cybersecurity teams and improving the combination of soft skills and technical skills. Several participants indicated that soft skills such as communication, detail-orientation, problem-solving, and empathy are typically more common workforce traits for women in their country.

    - Threat Mitigation: Increasing the diversity of ideas to help predict and prevent cyber threats.

- Inspire Future Generation: Increasing the reach of cybersecurity and cyber safety programs with women in cybersecurity roles helping to inspire girls and other women to take their digital security and safety seriously as well as building their aspiration and confidence to pursue cybersecurity training and career pathways. This in turn will also support women to more fully participate in the digital economy and drive economic growth.

- Break Stigmas: Helping to break stigmas around women's capabilities and role in society and challenges perceptions that only a man can complete more technical and specialist roles in the workforce.

- Increase Resource Base: Providing a larger resource base to draw from to help countries address cybersecurity workforce and skills gaps and support the full utilization of the labour market and the economic benefits that this would bring.

- In addition, the opportunities for benefits to be gained by women themselves in entering the cybersecurity workforce included:

    - Salary: Securing roles in a profession that has higher than average salaries.

    - Familial Stability: Cybersecurity is seen as a career with strong long-term prospects that can drive economic development for women and increase familial stability through flexible working.

Defined Future Workforce Roles and Training Pathways

Chapter three provided an understanding of the technical cybersecurity workforce job roles and associated skills required across all involved organisations for the five research focus countries to fulfil their digital transformation and cybersecurity capacity development ambitions and respond to and mitigate the risk from the growing cyber threat landscape.

- Utilising an existing Cybersecurity Skills Framework, the Future Workforce Assessment mapped priority technical cybersecurity roles that will be important in responding to the strategic drivers outlined in Chapter one.

- In addition, five technical cybersecurity roles were identified as starting points that countries might consider when approaching the development of their workforce.

- Through clearly identifying and defining priority technical cybersecurity roles, there is an opportunity for countries to develop informed (and perhaps combined) workforce development policies and activities as well as interventions specifically targeted at increasing the participation in the cybersecurity workforce such as raising awareness of specific cybersecurity roles, building aspiration for a range of cybersecurity career pathways, clearly defining job role requirements, and mapping education and training pathways that will equip prospective cybersecurity professionals with the knowledge, skills, and abilities to pursue a successful cybersecurity career.

Building on existing Education and Training Market

Chapter four presented a market assessment of the current cybersecurity skills base in each of the five research focus countries.

- The market assessment found that at least one university in each country offers a cyber-specific degree at both undergraduate and postgraduate level, with many more offering computer science and information technology degrees with cybersecurity modules.

- In addition, private groups and online academies were identified as the key providers of professional certifications. These groups provide support to both individuals and commercial entities.

- Regional and international organisations, as well as private groups, are also the main providers of female-focused initiatives in the region, with Indonesia and Thailand being the only two countries in the study to have gender-based initiatives in the sector. The UN, Australia and Microsoft emerged as significant stakeholders in increasing cyber literacy among women.

- With cybersecurity already established as part of the education and training market across the five research focus countries, there is an opportunity to build on this foundation and explore efforts to incorporate female-focused initiatives as part of this growth strategy.

Challenges

Barriers to Participation

Chapter two presented insights on the participation of women in the cybersecurity workforce in the Southeast Asian region and explored topics including identifying barriers that need to be addressed to improve female participation rates including:

- Societal Expectations: Societal expectations of women's role in family and pressure to leave the workforce if they get married, have children, need to look after a parent, all of which then impacts hiring choices for employers. Also, in some cases when families have limited resources and multiple children, they might prioritise sending a son to university instead of their daughter as they expect this will provide a greater economic benefit to the family.

- Gender Perceptions: Perceptions that boys are generally better with computers, discouraging girls to participate in related activities during schooling and ingraining notions that more technical study areas are too hard for woman.

- Discrimination: Women are currently the minority in cybersecurity training classes and face discrimination and isolation during their study.

- Cost: There is often a high cost to complete cybersecurity training courses or university study and women often rely on scholarships to pursue such education pathways.

- Access to Promotions: Even when women make it into cybersecurity roles that have trouble gaining promotions to senior and leadership roles due to stereotypes that men are better suited for such positions.

- Low Visibility: With less women in the cybersecurity workforce there is less visibility for aspiring professionals to see role models that they can aspire to and talk with to gain confidence and build aspiration to pursue their own cybersecurity career.

- Hiring Practices: Instances where job advertisements for cybersecurity roles specific that they are looking for male candidates.

Limited Female-Focused Education and Training Initiatives

Chapter four presented a market assessment of the current cybersecurity skills base in each of the five research focus countries.

- Affirmative action gaps in higher education: Research indicates that whilst women sit on the faculties of institutions offering cybersecurity degrees, none of them provide gender-based initiatives to increase women's access to higher education in the field.
- Incentive gaps in the public sector: Research also identified significant gaps in female-focused and gender-based initiatives in the public sector in all countries. International organisations are the key providers of these, though the programmes often target specific demographics - either civil servants or MSMEs – leaving significant gaps in the market.
- Gaps in private sector initiatives: Private sector entities do not engage in any specific female-focused initiatives, thus increasing barriers of access to vocational training and professional certifications.

The Need for Scale and Validation to address Gaps in the Education and Training Market

Chapter five produced an assessment of the gap between the anticipated skill requirements and current skills and training capability and capacity across the five research focus countries. The gap assessment focused on the five priority technical cybersecurity roles identified as starting points for consideration in the future workforce assessment.

- Limited offer in cybersecurity education and training: This gap assessment found that in most instances cybersecurity education and training offerings for the five priority technical cybersecurity roles exists but is currently very narrow and not sufficient to support expected future workforce and skills requirements.
- Gaps in education and training for senior roles: In terms of additional workforce requirements, with the exception of Thailand, the assessment was unable to identify sufficient existing cybersecurity education and training provisions or capabilities to support the broader skills development for Senior Executives, Managers and IT Staff. These are significant gaps as senior staff are needed to be able to develop and embed cybersecurity strategies and policies as part of a cybersecurity culture, supported by managers who can apply organisational policies across their teams. The research also identified that there is a gap in training provisions across the region for IT Staff who perform vital roles for organisations in being able to respond to and investigate cyber incidents.
- Narrow market access for women: Such limitations in the market are contributing to the access challenges for women in pursuing cybersecurity education and training opportunities.

Recommendations

Reflecting on the analysis of the research findings, including the challenges and opportunities for women's participation in the cybersecurity sector across Cambodia, Indonesia, Laos, Mongolia and Thailand, this section offers key recommendations for future capacity building programs in this field across these five geographies, as well as intervention approaches that can amplify the inclusion of women in this field.

Recommendations for Capacity Building Intervention Design Strategies

As the research has demonstrated, promoting the participation of women in the cybersecurity sector is a multi-faceted issue that requires complementary and mutually reinforcing approaches to address the issue in a meaningful and effective way. To this end, when considering capacity building interventions in this field, it is recommended to utilise the following strategies:

R1 - Interventions that Pursue an Ecosystem Approach

When developing capacity building interventions focused on increasing the participation of women in the cybersecurity workforce, it is important to consider the full ecosystem in which such interventions will be deployed and the outcomes such interventions are expected to deliver. Based on the research findings outlined in this report, the cybersecurity workforce development ecosystem for the participation of women includes the following eight interconnected elements:

1. Awareness and Aspiration

In order for girls and women to pursue cybersecurity careers it is crucial that they are informed and inspired about cybersecurity careers from an early age and that opportunities for growth and development are communicated throughout their careers. As such, cybersecurity awareness interventions starting at primary school level onwards are an important element to support the participation of women in the cybersecurity workforce. The earlier this occurs the more agency girls and women have to make decision and pursue opportunities that can support entry into the cybersecurity workforce. Such awareness and aspiration initiatives should focus not only on women and girls, but also key stakeholders that are likely to influence their education and career decision-making process such as parents, teachers, community leaders, professional associations, and employers to name a few.

2. Primary and Secondary School

The introduction of cybersecurity as a career and cybersecurity related academic content needs to occur during primary and secondary school stages in order for girls to develop the related STEM and Cybersecurity academic knowledge that will be necessary to successfully pursue post-secondary school cybersecurity education and training. Consideration should be given not just to the introduction of relevant curriculum and related activities, but to also creating engaging and inclusive environments that encourage girls to participate.

3. Tertiary Education

The availability of a range of education pathways leading to cybersecurity careers will increase the options and accessibility of cybersecurity careers for women (and all members of society). This might include formal cybersecurity programs at university and vocational providers as well as apprenticeships and other education pathways. Beyond the development and availability of such education programs, consideration needs to also be given to the entry requirements including academic as well as economic and socio-cultural factors that may form barriers for women. In addition, once women enter a program of study, consideration needs to be given to the inclusiveness of the study environment.

4. Training and Certification

As a complement to Tertiary Education pathways to cybersecurity careers, another key element is training and certification which can provide entry as well as advancement pathways. This includes formal training aligned to local and internationally recognised certifications that women can complete to demonstrate their qualifications for different technical cybersecurity roles. This also includes opportunities for informal on the job-training and mentoring that can be crucial for ongoing professional development and career progression. Consistent with the Tertiary Education element, such Training and Certification needs to consider issues of accessibility and inclusivity.

5. Recruitment and Hiring Practices

This element focuses on the entry process into the cybersecurity workforce for women and how the organisational job role design, entry requirements, recruitment approaches, and hiring decisions might influence the applications from and the success of female candidates.

6. Inclusive Work Environments

In order to attract and support women to enter the cybersecurity workforce, consideration needs to be given to their work environment to ensure women are provided opportunities to complete meaningful work, have access to flexible working arrangements that align with the local sociocultural context, and are able complete their jobs in respectful work environments.

7. Workforce Retention and Promotion

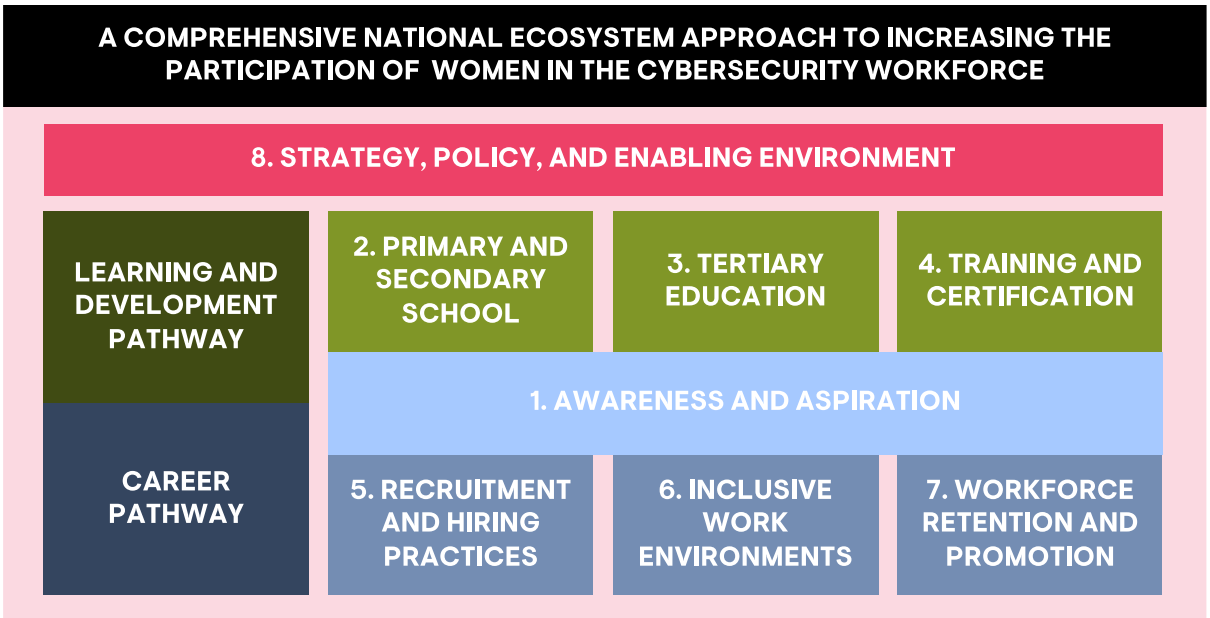
Building on the inclusive work environment outlined in element six, consideration needs to be given to the retention and advancement of women once they have successfully entered the cybersecurity workforce. This should consider both initiatives that support women's ability to balance their family and professional life, provide ongoing support and encouragement to participate in upskilling and continuing professional development programs, as well as clear pathways for career development, promotion, and inclusion of women in senior leadership roles within organisations.

8. Strategy, Policy, and Enabling Environment

All the elements elaborated above cannot be sustainable or effective in a bubble. It is critical to understand any gaps in the broader enabling environment of the national legal, regulatory, economic, and societal context for the participation of women and girls in education and workforce, and where possible to address them as part of the intervention. The enabling environment, consisting of laws, policies, power structures, business environment, and culture can also be understood as the conditions necessary for the sustainability and success of the change process pursued by the specific intervention to enhance the participation and role of women in cybersecurity in the national context. It is a critical component especially in interventions that address workforce development given that it is meant to support a functioning market economy as well as relevant policies that promote digital literacy, research and development, and a skilled workforce.

These eight elements defined above are illustrated below to show a comprehensive national ecosystem approach to increasing the participation of women in the cybersecurity workforce.

Figure 5 - Women in Cybersecurity National Ecosystem Approach



Examples of benefits from considering the national ecosystem approach in which capacity building interventions will be deployed include:

- Designing interventions that are informed by ecosystem gaps, as well as complement existing interventions already occurring in the ecosystem.
- Identifying the absorption capacity and any gaps in the ecosystem that might impact the success of a capacity building intervention and adjusting the timing or scope of programs to optimise chances of success.
- Reducing duplication of effort by scanning the ecosystem and ensuring new interventions build-on rather than replicate existing interventions.

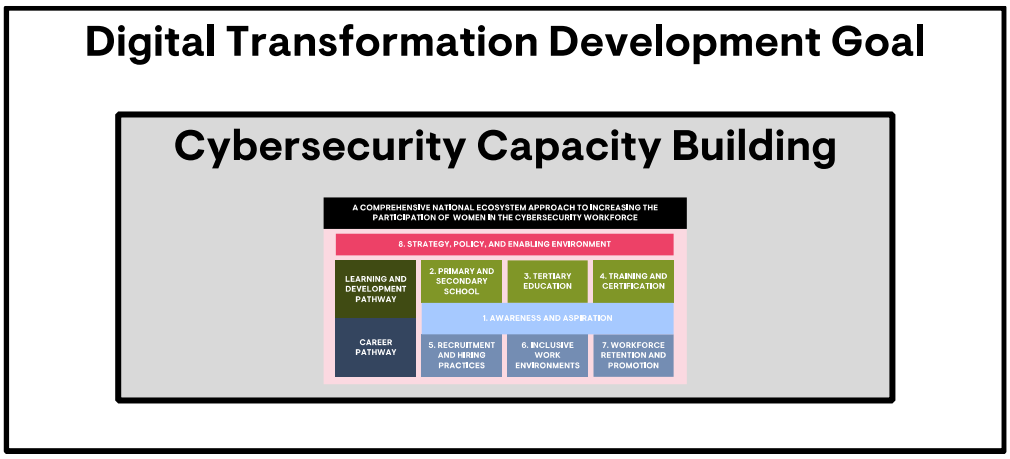
R2 - Interventions that Incorporate a Gender-Sensitive Dimension Within Digital Development

In light of the increased investment in digital development initiatives, it is important to utilize all opportunities for promoting a gender-sensitive approach in such initiatives and ensure they include components addressing the digital literacy and cybersecurity skills gaps through relevant education, skilling, reskilling, and upskilling activities that are responsive to the needs of women and girls.

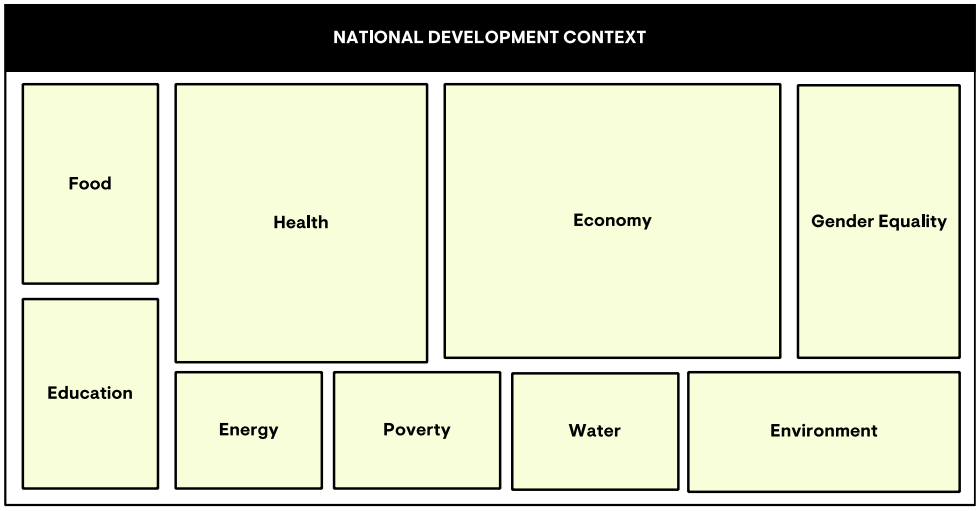
R3 - Interventions that Amplify Gender-Responsive Cybersecurity Capacity Building within the National Development Context

It is often the case that cyber capacity building interventions are pursued without a deliberate connection with the broader national development agenda. Yet, promoting the participation of women in the cybersecurity sector requires an understanding of a complexity of issues that lie at the intersection of the empowerment of women and girls, the national digital transformation journey, and the education and employment environment. This means that there is both an opportunity and a necessity to consider a systematic integration of gender-responsive approaches in cybersecurity and digital transformation actions as part of overall development objectives to deliver more equitable results for women and girls.

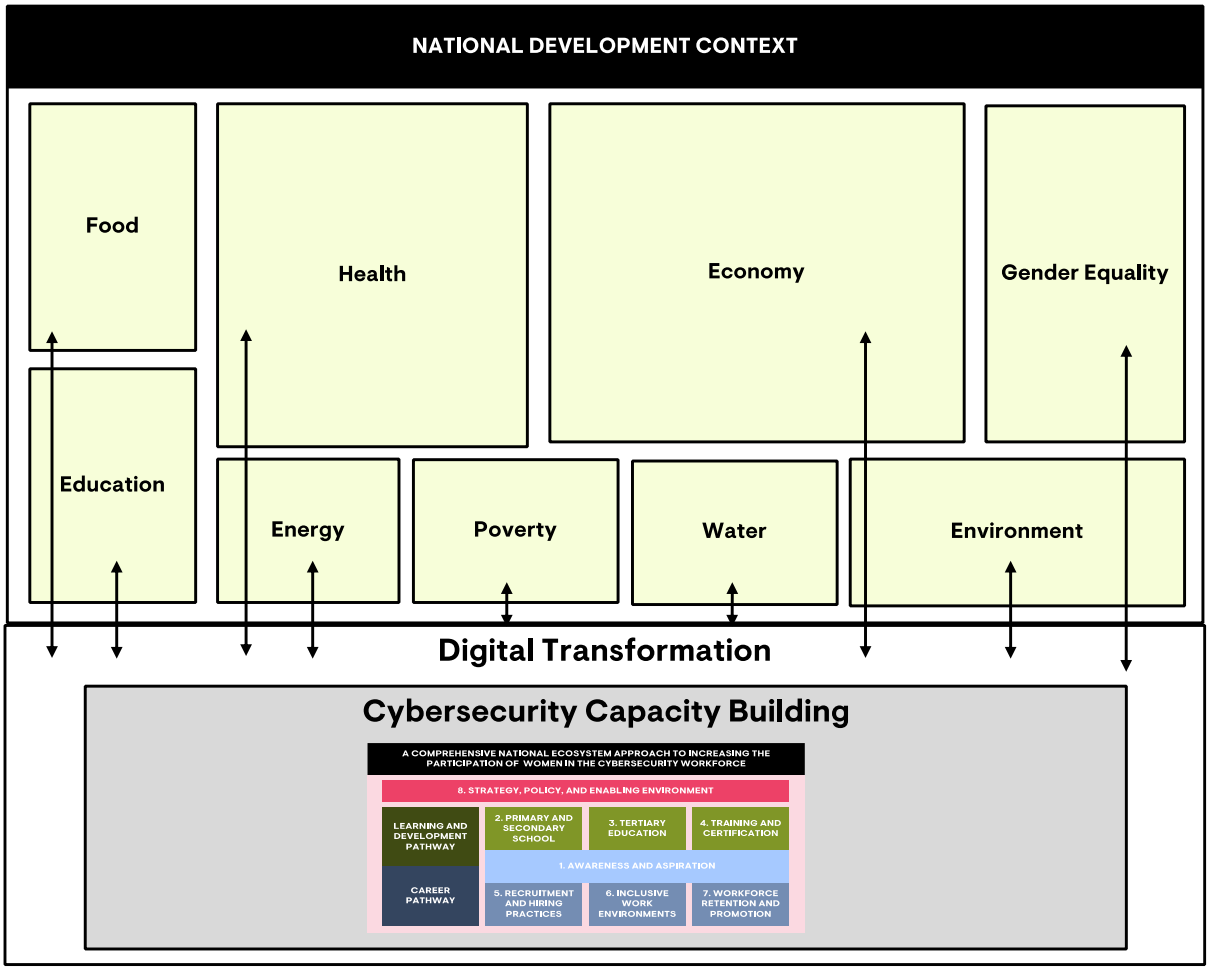
A high-level illustration of this is provided in the series of diagrams below where firstly it is recognised that a Women in Cybersecurity National Ecosystem Approach sits within the broader context of National Cybersecurity Capacity Building, which in itself is part of the Digital Transformation Development Goal of a given country.



Secondly is an example National Development Context (key areas and level of priority will be different for each national context) which illustrates a range of competing priorities that countries are typically simultaneously working on and trying to advance at a given time.



Bringing these together below, the next diagram shows that Digital Transformation efforts need to be integrated across the development context. As such, to optimise their impact and reach, capacity building efforts focused on the participation of women in the cybersecurity workforce need to be designed, implemented, and integrated as part of the national development context and its range of priority development areas.



Recommendations for Capacity Building Intervention Principles and Approaches

Further to the above-mentioned vertical intervention strategies, a combination of horizontal principles and approaches across development interventions can enhance the meaningful promotion and inclusion of women in the cybersecurity sector.

R4 - Co-Design Interventions to Foster Sustainable, Locally-led Change

The significance of local ownership in the design and implementation of development interventions is long established (see most recently the 2022 Donor Statement on Supporting Locally Led Development led by USAID[374]). In the case of women in cybersecurity, it is necessary to consider how to support co-created and locally-led interventions that build on local knowledge, capacity, and expertise and integrate collaborative efforts that address the context-specific barriers that women face in accessing and pursuing cybersecurity education and workforce opportunities. The creation and development of local cybersecurity ecosystems that also promote female leadership and entrepreneurialism is a key part in this equation.

R5 - Pursue Public-Private Partnerships and Whole-of-Society Approaches

Skills and workforce development are areas of intervention that by default require a collaborative approach within government and across society. Pursuing a whole-of-society approach that leverages the investment and expertise of government, the private sector, civil society, academia, and the

[374] https://www.usaid.gov/localization/donor-statement-on-supporting-locally-led-development

research community is a starting point for all workforce initiatives which need to be informed by the local context and the gender specificities.

R6 - Balance between Short-Term and Longer-Term Intervention Approaches

When building and shaping a national workforce pipeline, there is a need to balance investments on both immediate needs and changes through targeted shorter-term interventions as well as investing in longer-term changes that will impact whole cohorts of women over time. Short-term interventions can target 'low hanging fruit' and immediate gaps that need to be addressed via targeted interventions at specific points in the Women in Cybersecurity National Ecosystem. Longer-term interventions can support whole future cohorts of women as they move throughout their learning and development and career pathways and focus on sustainability and larger scale impact over time. Including both short-term and longer-term focused interventions needs to be considered as part of overall programming efforts.

R7 – Account for the impact of broader systemic barriers to women's participation the Cybersecurity workforce

As noted in Recommendation 3, the participation of women in the cybersecurity workforce needs to be considered as part of the national development context. As part of this, the design of capacity building interventions needs to take into account the broader systemic barriers to women's participation in education and training and the workforce that will influence their ability to pursue cybersecurity as a profession. Whilst cybersecurity capacity building efforts cannot be expected to address all systemic barriers in a country it is important that such efforts consider and mitigate where possible the impact of these barriers as well as ensuring they make a positive contribution to the broader gender equality goals of the country.