



Australian Government

Department of Foreign Affairs and Trade



CADT

បណ្ឌិត្យសភាបច្ចេកវិទ្យាឌីជីថលកម្ពុជា

Cambodia Academy of Digital Technology

Cambodian Cyber Security Capability Assessment

Prepared by CyberCX on behalf of the
Cambodian Government and supported by
the Australian Department of Foreign
Affairs and Trade

APRIL 2022

VERSION 1.0



Cambodian Cyber Security Capability Assessment

VERSION 1.0

APRIL 2022

CyberCX

CYBER SECURITY + CUSTOMER EXPERIENCE

Revision History

Version	Revision Description	Date
0.1	Cambodian Cyber Security Capability Assessment Report Initial Draft	11/11/2021
0.2	Refining scope and progress feedback	14/12/2021
0.3	General feedback and suggested changes	25/01/2022
0.4	Internal detailed review and suggested changes round one	10/02/2022
0.5	Internal detailed review and suggested changes round two	22/02/2022
0.6	Internal detailed final review and minor changes	01/03/2022
0.7	Socialisation with DFAT Cambodia	01/03/2022
0.8	Incorporation of feedback from DFAT Cambodia	21/3/2022
1.0	Submission to MPTC	4/4/2022

Table of Contents

1	Executive Summary	6
2	Background	7
2.1	Initiative	7
2.2	History of Cambodia's Cyber Security.....	7
2.2.1	Incidents	7
2.2.2	Legislation and Frameworks	8
3	Cambodian Cyber Context.....	10
3.1	National Cyber Legislation and Initiatives.....	10
3.2	Bilateral.....	11
3.3	Multilateral.....	12
4	Cyber Security Capability Assessment	13
4.1	Framework	13
4.2	Maturity Level	14
5	Methodology.....	15
6	Initial Findings	16
6.1	Documentation Review	16
6.2	Key Themes from Stakeholder Interviews	17
7	Cyber Security Capability Analysis and Assessment.....	19
7.1	Cluster 1 - Cyber Security Governance and Standards	19
7.1.1	Establish Baseline Security Measures.....	19
7.1.2	Roles and Responsibilities.....	21
7.2	Cluster 2 - Capacity-building and Awareness	23
7.2.1	Training and Education	24
7.2.2	User Awareness.....	25
7.2.3	Research & Development	27
7.3	Cluster 3 - Legal and Regulatory	29
7.3.1	Protection of Critical Information Infrastructure	29
7.3.2	Incident Reporting Framework	31
7.4	Cluster 4 - Cooperation	33
7.4.1	Inter-Ministry Cooperation	33
7.4.2	International Cooperation.....	35
7.5	Cluster 5 - Targeted Incident Response.....	37
7.5.1	Operational Capabilities and Institutionalised Systems	37
8	Future Capability and Roadmap	40
8.1	Cyber Security Governance and Standards.....	41
8.2	Capacity-building and Awareness	43
8.3	Legal and Regulatory.....	46
8.4	Cooperation	48
8.5	Targeted Incident Response.....	50
9	About CyberCX.....	52
10	Appendices	53
	Appendix A Cyber Security Capability Survey Questions	53
	Appendix B Relevant Engagements In The Region.....	62

Appendix C	Bibliography.....	63
------------	-------------------	----

Index of Tables

Table 1 - Cambodian Cyber Security Capability Assessment Clusters and Sub-sections.....	14
Table 2 - Maturity Levels and Definitions.....	14

Index of Figures

Figure 1 - Question 13 Survey Results	20
Figure 2 - Question 14 Survey Results	22
Figure 3 - Question 17 Survey Results	24
Figure 4 - Question 16 Survey Results	26
Figure 5 - Question 19 Survey Results	28
Figure 6 - Question 21 Survey Results	30
Figure 7 - Question 22 Survey Results	30
Figure 8 - Question 24 Survey Results.....	32
Figure 9 - Question 7 Survey Responses	34
Figure 10 - Question 9 Survey Responses	36
Figure 11 - Question 26 Survey Responses	38
Figure 12 - Question 28 Survey Responses	38
Figure 13 - Question 29 Survey Responses	39
Figure 14 - Cyber Security Resilience Roadmap	40

1 Executive Summary

Context

CyberCX has been engaged by the Department of Foreign Affairs and Trade as part of the Cyber and Critical Tech Cooperation Program, to support the strengthening of Cambodia's cyber security institutions and resilience in a two-phased project. Phase 1 constitutes an assessment of the Cambodian Government's cyber security capabilities. Phase 2 includes the design and implementation of cyber security education and training for Cambodian Government Ministries and their staff.

Aim

The purpose of this report is to establish a comprehensive and accurate understanding of the Cambodian Government's current cyber security capability and maturity. The findings from this report will influence the design of customised cyber security training and education to be delivered to Cambodian Government Ministry staff in 2022.

Method

Extensive desktop research, stakeholder interviews with Cambodian subject matter experts, and a Cyber Security Capability Survey distributed to Government Ministry staff was conducted to gather quantitative and qualitative information on previous and existing cyber security capability.

Findings

The Cyber Security Capability Assessment identified numerous key findings. Across the five cyber security cluster categories, seven sub-sections out of ten were assessed as *Maturity Level 2 – Early Definition*. Key points included:

- Cyber security legislation is in development. However, this is challenging due to difficulties in translating technical jargon into Khmer. Senior Government policymakers also have limited understanding of cyber security threats and their potential implications for Cambodia's national interests. This limits their contextual understanding of the drivers behind cyber security legislation.
- Cyber security awareness and understanding is limited across all levels of Ministry staff, including junior and executive level personnel.
- Inter-Ministry cooperation exists. However, findings showed that it occurs irregularly, without holistic appreciation for complex cyber security topics.

Recommendations

Based on research conducted, 19 recommendations have been identified for consideration and prioritisation by the Cambodian Government for future implementation in the short, medium, and long term. Two recommendations are intended to be implemented and supported by CyberCX in Phase 2 of the project. They are:

- **Objective 2.0:** Delivery of a cyber security awareness program to selected Cambodian Government staff and Trainers
- **Objective 5.0:** Delivery of cyber security incident response technical training

2 Background

CyberCX has been engaged by the Australian Government's Department of Foreign Affairs and Trade (DFAT) as part of its Cyber and Critical Tech Cooperation Program (CCTCP) to strengthen Cambodia's cyber security institutions and resilience in a two-phased project. Phase 1 includes the development of a Cyber Security Capability Assessment, describing the Cambodian Government's current cyber security posture and a roadmap to uplift Cambodia's cyber security capabilities. Phase 2 includes the delivery of training to Cambodian Government stakeholders to uplift key cyber skills identified in the initial Cyber Security Capability Assessment.

2.1 Initiative

Australia's former Foreign Minister, The Hon Julie Bishop, launched Australia's first International Cyber Engagement Strategy (the Strategy) on 4 October 2017. The Strategy focussed on maintaining an open, free, and secure internet that protects national security and promotes international stability while driving economic growth and sustainable development.¹ The Strategy introduced Australia's CCTCP initiative which aims to partner with countries in the Indo-Pacific region to support the uplift of cyber resilience and provide countries with the capability to take advantage of the opportunities that an open, free, and secure cyberspace presents. The Strategy aims to achieve cyber resilience through the enhancement of cyber security knowledge and practices. This includes building the capability to defend against cybercrime, enhanced respect for human rights and democratic values, and the online resources needed to advance and protect global interests in cyberspace.²

2.2 History of Cambodia's Cyber Security

The internet was introduced to mainstream Cambodia in 2001 with the acquisition of their Internet Protocol (IP) address delegation from the Asia Pacific Network Information Centre.³ After this, the number of Internet Service Providers (ISPs) in Cambodia grew significantly to accommodate the spread of the internet.⁴ Currently, there are six mobile ISPs and 11 fixed internet service companies in Cambodia.⁵ Internet connectivity is now widespread throughout Cambodia with 98.5% of the population having access to the internet.⁶

2.2.1 Incidents

Since the internet was introduced to Cambodia, Government Ministries, politicians, businesses, armed forces, and the Cambodian public have all been the target of cyber-attacks.⁷ Notable incidents occurred in 2012, 2018, and 2020.

In 2012, the co-founder of *The Pirate Bay* was arrested by Cambodian authorities and deported. In response, two international hacking groups executed cyber-attacks on the Cambodian

¹ 'Australia's International Cyber and Critical Tech Engagement Strategy', April 21, 2021, Commonwealth of Australia, Department of Foreign Affairs and Trade.

² Ibid.

³ Michael Minges, Vanessa Gray, and Lucy Firth, March 2002, 'Khmer Internet: Cambodia Case Study', International Telecommunication Union Geneva Switzerland.

⁴ 'Leveraging Investments in Broadband for National Development: The Case of Cambodia', 2018, UN-OHRLLS.

⁵ Ibid.

⁶ Spokesman of TRC, October 2021, 'Mobile Internet Subscribers 2021 (Oct)', Telecommunication Regulator of Cambodia, <https://www.trc.gov.kh/en/internet-subscribers/>.

⁷ Somaly Nguon, and Sopheak Sun, January 2020, 'Cambodia v. Hackers: Balancing Security and Liberty in Cybercrime Law', Konrad Adenauer Stiftung.

Government.⁸ The first group targeted Cambodian businesses, the Government, and armed forces, and leaked highly confidential information.⁹ The second group leaked 5,000 Government files, including sensitive documents about drug trafficking authorities from the Ministry of Foreign Affairs, on the dark web.¹⁰

In November 2018, several of Cambodia's biggest ISPs were hit by distributed denial-of-service (DDoS) attacks over several days.¹¹ As a result, ISP users had difficulty accessing online services for an entire week. Affected ISPs were unable to provide sufficient DDoS mitigation services to safeguard their infrastructure, forcing them to outsource support during the attacks.¹²

More recently, in December 2020 the Cambodian Ministry of Posts and Telecommunications (MPTC) reported that cybercriminals had used fake accounts mimicking senior Government officials on the social media application Telegram, to send files and links containing malware to victims.¹³ This phishing scam targeted the Cambodian public and provided cybercriminals with remote access to victims' devices.

The progression of these cyber incidents demonstrates the increasing sophistication of cyber threats to both the Cambodian Government and the public.

2.2.2 Legislation and Frameworks

The Cambodian Government is in the process of developing legislation and frameworks to support the growing influence and importance of technology in Cambodian society, and to ensure that Cambodia's national interests are protected.

Cambodia's ICT Masterplan (the Plan) was published in 2014 to support the crucial role Information and Communications Technology (ICT) plays in enabling Cambodia's development. It presents a roadmap highlighting standards required to take advantage of secure ICT opportunities. The Plan focuses on four strategic drivers:

1. Enriching e-services
2. Empowering people
3. Ensuring connectivity
4. Enhancing capabilities

The Plan's objectives were not reached by the proposed 2020 target. Despite this, Cambodia has made significant progress since 2014. Ongoing objectives include reaching the top 50 ranking countries of the ICT-related World Economic Forum (WEF) index.¹⁴ In the 2019 ICT-related WEF index, Cambodia ranked 71st for its ICT adoption.¹⁵

The Cambodian Criminal Code (the Code) was published in 2009 and defines 'Offences Related to Information Technology'. It determines parameters for guilt, sets penalties for breaching the law, and describes how laws will be enforced.¹⁶ The Code sets out four main articles of offences relating to information technology:

⁸ Ibid.

⁹ Nguon and Sun, January 2020, 'Cambodia v. Hackers'.

¹⁰ Ibid.

¹¹ Catalin Cimpanu, November 8, 2018, 'Cambodia's ISPs hit by some of the biggest DDoS attacks in the country's history', ZDNET, <https://www.zdnet.com/article/cambodias-isps-hit-by-some-of-the-biggest-ddos-attacks-in-the-countrys-history/>.

¹² Ibid.

¹³ Taing Rinith, December 17, 2020, 'MPTC warns of hackers' attack on Cambodian Telegram users', Khmer Times, <https://www.khmertimeskh.com/50794217/mptc-warns-of-hackers-attack-on-telegram-users/>.

¹⁴ 'Summary on Cambodian ICT Masterplan 2020', 2014, Korea International Cooperation Agency (KOICA).

¹⁵ Klaus Schwab, October 2019, 'Global Competitiveness Report 2019', World Economic Forum.

¹⁶ Bunleng Cheung, November 2009, 'Criminal Code: Khmer-English Translation', Kingdom of Cambodia. 183-186.

- Unauthorised access to automated data processing systems
- Obstructing the functioning of automated data processing systems
- Fraudulent introduction, deletion, or modification of data
- Participation in a group that conspires to commit offenses and/or conspiracy to commit offences¹⁷

In 2015 Cambodia implemented the Law on Telecommunications (the Law). The Law established the authority of MPTC for cyber security-related issues and is applied to all telecommunication operations in Cambodia.¹⁸ The purpose of the Law is to:

- Ensure the provision of effective, safe, high quality, reliable, and affordable telecommunication infrastructure, networks, and services in response to the needs of social and economic development in Cambodia
- Ensure the development and governance of the telecommunications sector, including regulation of telecommunication operators and persons involved with the telecommunications sector, and lawful and fair competition to enhance mobilisation of national revenue and protect subscribers
- Ensure the protection of users and mobile revenues for the National Budget¹⁹

At time of writing, the Plan, the Code, and the Law are the main, existing pieces of legislation supporting cyber security in Cambodia. The Cambodian Government is currently developing new cyber security legislation, which is discussed in detail in Section 3.1 of this document.

¹⁷ Cheung, November 2009, 'Criminal Code'.

¹⁸ 'Law on Telecommunications', November 2015, Kingdom of Cambodia.

¹⁹ Ibid.

3 Cambodian Cyber Context

3.1 National Cyber Legislation and Initiatives

The Cambodian Government is in the process of developing new legislation and frameworks to support the growing integration of technology into life in Cambodia. Four supporting pieces of legislation and/or frameworks are currently being developed:

1. The Cybercrime Law
2. The Cyber Security Law
3. The Personal Protection Law
4. The Digital Government Framework

Development of The Cybercrime Law 2012 (the Cybercrime Law) by the Ministry of Interior began after the 2012 cyber-attack on Cambodian businesses, Government, and armed forces.²⁰ The Cybercrime Law gained international attention due to the enforcement of penalties for people who “establish contents deemed to hinder the sovereignty and integrity of the country, of Government agencies or Ministries, incite or instigate, generate insecurity and political discord and damage the moral and cultural values.”²¹ Infringement of this law is punishable by one to three years imprisonment and heavy fines.²² Since initial development, redrafting of The Cybercrime Law has been stopped, as it could be interpreted too broadly and poses the risk of infringing fundamental rights.²³

MPTC are currently working on a range of legislation to enforce and encourage critical infrastructure providers and the broader community to prioritise cyber security. These include planning for the Personal Protection Law in Cambodia, the Digital Governance Framework, and the Cyber Security Law. The Digital Government Framework aims to support the Cambodian Government’s development of e-Government services for the public that are secure and easily accessible. Stakeholder interviews highlighted MPTC’s involvement in developing the Cyber Security Law and the Personal Protection Law, however, no further information about this legislation was gathered during the research phase of this report.

A common challenge for Cambodian Government Ministries developing cyber security legislation and frameworks is communication barriers regarding the translation of technical jargon for senior Government policymakers. Often when Government Ministries approach senior Government policymakers to discuss the importance of cyber security, understanding of relevant threats and potential implications for Cambodia’s national interests is insufficient and its importance is downplayed.

The National Internet Gateway (NIG) is an initiative being established by the Cambodian Government to facilitate and manage domestic and international internet connections.²⁴ The Cambodian Government has stated that the system will be used to boost revenue collection, better regulate internet providers and tackle cybercrime.²⁵ It will consist of two exchanges: the Domestic Internet Exchange that will be used for the exchange of domestic Internet data and the International Internet Gateway which will be used for the exchange of Internet data domestically

²⁰ Nguon and Sun, January 2020, ‘Cambodia v. Hackers’.

²¹ Article19, 2014, ‘Cybercrime Law’, Kingdom of Cambodia. https://www.article19.org/wp-content/uploads/2018/02/Draft-Law-On-CyberCrime_Englishv1.pdf

²² Ibid.

²³ Nguon and Sun, January 2020, ‘Cambodia v. Hackers’.

²⁴ Royal Government Kingdom of Cambodia, February 16, 2021, “Sub-Decree on Establishment of National Internet Gateway,” Digital Reach Asia. https://digitalreach.asia/wp-content/uploads/2021/06/Cambodia_NIG_English.pdf.

²⁵ Turton, Shaun, February 15, 2022, “Cambodia postpones ‘national internet gateway’ plan due to COVID,” NIKKEI Asia. <https://asia.nikkei.com/Spotlight/Society/Cambodia-postpones-national-internet-gateway-plan-due-to-COVID>.

and internationally.²⁶ It will be operated by NIG Operators who will be determined by the Royal Government according to the requests of MPTC.²⁷ However, the NIG initiative has been postponed by the Cambodian Government due to COVID.²⁸

3.2 Bilateral

The Cambodian Government has established partnerships with multiple countries in the Indo-Pacific region including India, Japan, Australia, and Association of Southeast Asian Nations (ASEAN) members and has developed initiatives dedicated to strengthening its cyber security posture and capabilities.

India supports the uplift of Cambodian information technology through the Mekong Ganga Cooperation Initiative. This initiative provides Quick Impact Projects on IT which have doubled each year since 2019.²⁹ Stakeholders from the Cambodian Academy of Digital Technology (CADT) noted during interviews that the Indian Government facilitates training programs for educational instructors from CADT to strengthen their cyber security courses.

Japan provides cyber security capacity-building support to Cambodia through the ASEAN Japan Cyber Security Capacity Building Centre.³⁰ Capacity-building activities include cyber security exercises, awareness raising, cyber security metrics and critical information infrastructure protection.³¹ Japan is a strategic partner for Cambodia to work with as it continues to strengthen its cyber security posture and capabilities.

Cambodia and Australia have a strong bilateral partnership which has been strengthened by the COVID-19 Global Pandemic (COVID-19). Australia has supported Cambodia to address the social and economic impacts of the pandemic, positively influencing and supporting Cambodia's COVID-19 recovery and growth moving forward.³² The Cambodian Cyber Security Uplift project is being delivered through the DFAT CCTCP. CCTCP is partnering with ASEAN and Pacific Island countries to support targeted, cyber security capacity-building that will enable them to respond to cyber and critical technology-related challenges and opportunities. The outcomes of this project include strengthening and establishing frameworks to support capability growth, fostering regional collaboration, and increasing awareness of cyber security and digital technologies.

Stakeholder interviews highlighted that, before COVID-19, the Cambodian Government had partnered with the Japanese and South Korean Governments to provide joint training to strengthen staff cyber security capability and knowledge. MPTC noted that all Cambodian Government Ministries showed interest in attending these joint training programs. Joint training programs can take several forms. For example, 'Train the Trainer' programs were hosted by Japan and South Korea for Cambodian Government IT training staff. This program provided training staff with opportunities to develop and update their knowledge and skills, to then share and re-teach to colleagues and wider Ministry staff. In addition, the Japanese Government has provided support to the Cambodian Government to use international cyber security standards for IT systems, such as

²⁶ Royal Government Kingdom of Cambodia, February 16, 2021, "Sub-decree on the establishment of the National Internet Gateway".

²⁷ Ibid.

²⁸ Turton, February 15 2022, "Cambodia postpones 'national internet gateway' plan due to COVID".

²⁹ 'India-Cambodia Bilateral Relations', February 5, 2020, Indian Ministry of External Affairs.

https://www.mea.gov.in/Portal/ForeignRelation/India-Cambodia_Bilateral_Brief_feb_2020.pdf

³⁰ 'Outcomes of the 14th ASEAN-Japan Cybersecurity Policy Meeting', October 22, 2021, Ministry of Economy, Trade and Industry. https://www.meti.go.jp/english/press/2021/1022_001.html.

³¹ Ibid.

³² 'Development assistance in Cambodia', Department of Foreign Affairs.

<https://www.dfat.gov.au/geo/cambodia/development-assistance/development-assistance-in-cambodia>.

the Centre for Internet Security benchmarks, which are translated into Khmer. In addition, Japan has provided funding for cyber security research projects through the United Nations.

The importance of building Cambodia's bilateral partnerships for cyber security capacity-building is discussed further in Sections [7.2.1](#) and [7.4.2](#).

3.3 Multilateral

Cambodia is one of the ten member states of ASEAN.³³ ASEAN member states aim to support regional prosperity, security, and growth, and, more recently, there has been an increased focus on transitioning the Southeast Asian region into a digital community.³⁴

ASEAN recently announced its vision to develop the region into a leading digital economy and society. The ASEAN digital community vision will be enabled through the integration of secure and transformative digital services, technologies, and ecosystems.³⁵ This vision seeks to empower individuals, businesses, and trade, focussing on the recovery of the economy after COVID-19.³⁶ As a consequence of the increased focus on digital community, ASEAN's risk of cyber-attack has increased.

To enable the vision of the region as a digital community, ASEAN has received support from Australia and its other allies. Australia and ASEAN have developed a partnership for this digital enablement which encompasses technical, policy and legislative support. In terms of technical partnership, the Australian Cyber Security Centre has partnered with ASEAN's top incident responders to compete in exercises. The focus of these exercises is to strengthen regional cyber defences and regional cooperation. Such initiatives are supporting the uplift of ASEAN's cyber resilience to enable ASEAN's transition towards a digital community.

The importance of building Cambodia's multilateral engagement on cyber security capacity-building is discussed further in Section [7.4.2](#).

³³ 'ASEAN Digital Masterplan 2025', 2020, The Association of Southeast Asian Nations.

³⁴ Ibid.

³⁵ Ibid.

³⁶ Ibid.

4 Cyber Security Capability Assessment

4.1 Framework

The European Agency for Cyber Security (ENISA) provides internationally recognised frameworks for enhancing and building national cyber security capabilities.³⁷

This Cyber Security Capability Assessment is aligned to the ENISA National Capabilities Assessment Framework (the ENISA Framework). The ENISA Framework (published in 2020) assists in identifying current maturity levels and capabilities as well as providing guidance on areas for improvement and further capacity development.³⁸ The ENISA Framework additionally enables entities to self-assess the maturity of their strategic and operational cyber security capabilities.³⁹

This Cyber Security Capability Assessment adopts the four clusters of the ENISA Framework relevant to Cambodia's cyber security context:

1. Cyber Security Governance and Standards
2. Capacity-building and Awareness
3. Legal and Regulatory
4. Cooperation

Targeted Incident Response is an additional cluster which has been included, as it was identified by Cambodian stakeholders as a key area to strengthen across Government.

The five clusters include specific sub-sections tailored to the Cambodian context for the purposes of this Cyber Security Capability Assessment (Table 1). The associated objectives have been designed to support identification of maturity levels.

Cluster and Sub-sections	Example Questions
Cyber Security Governance - Baseline Security Measures - Rolls and Responsibilities	- Does Cambodia have clearly defined processes and actions for handling cyber security crises? - Does Cambodia have an established cyber security baseline for capabilities and practices?
Capacity-building and Awareness - Training and Education - User Awareness - Research and Development	- Does Cambodia promote cyber security training and education aligned with national requirements? - Has Cambodia identified gaps in cyber security knowledge and developed a plan to raise/strengthen awareness? - Does Cambodia encourage and foster research and development on cyber security vulnerability causes?
Legal and Regulatory - Protection of Critical Information Infrastructure - Incident Reporting Framework	- Has Cambodia identified critical information infrastructure and mitigated the relevant risks? - Does Cambodia have a framework to assess the impact of incidents, assess vulnerabilities and update security measures?
Cooperation - Inter-Ministry Cooperation - International Cooperation	- Does Cambodia have institutionalised cooperation on cyber security between ministries with clearly defined responsibilities? - Does Cambodia benefit from a common knowledge base between ASEAN members and regional partners?

³⁷ Anna Sarri, Pinelopi Kyranoudi, Aude Thirriot, Federico Charelli, and Yang Dominique, 'National Capabilities Assessment Framework', December 2020, European Union Agency for Cybersecurity. DOI: 10.2824/590072.

³⁸ Ibid.

³⁹ Ibid.

Targeted Incident Response

- Operational Capabilities and Institutionalised Systems

- Does Cambodia carry out cyber security incident identification and triage, initial analysis, response and remediation, and digital forensic and incident response?

Table 1 – Cambodian Cyber Security Capability Assessment Clusters and Sub-sections

4.2 Maturity Level

The ENISA Framework suggests that the maturity level of a nation's cyber security capability should be assessed using an incremental five-point scale where Level 1 refers to limited, initial capability and Level 5 refers to dynamic and comprehensive capability (see Table 2). These levels have been tailored to encompass Cambodian contextual and cultural factors. The five levels represent stages that an entity may transition through when building cyber security capabilities across from the clusters articulated in Section 4.1. They have been deployed in this Cyber Security Capability Assessment to support maturity level assessment for Cambodian Government cyber security.

Maturity Level	Outline
Level 1 – Initial/Ad Hoc	- Does not have a clearly defined approach to building capacity in the corresponding cyber security cluster - Has generic goals in place and has performed some studies to improve national capabilities
Level 2 – Early Definition	- The national approach to capacity-building for clusters is defined - Action plans or activities to reach results are in place but at an early stage in development - Active stakeholders may have been identified and/or engaged
Level 3 – Establishment	- The action plan for capacity-building in clusters is clearly defined and supported by related stakeholders - Practices and activities are enforced and implemented uniformly at a national level - Activities are defined and documented with clear resource allocation, governance and deadlines
Level 4 – Optimisation	- Action plan is assessed on a regular basis; it is prioritised, optimised, and sustainable - Performance of cyber security capacity-building activities is regularly measured. - Success factors, challenges, and gaps in the implementation of activities are identified
Level 5 – Adaptiveness	- The cyber security capacity-building strategy is dynamic and adaptive - Constant attention to environmental developments (technological, advancements, global conflict, new threats etc) fosters a rapid-decision capability and an ability to act quickly for improvement

Table 2 – Maturity Levels and Definitions

5 Methodology

Information for this Cyber Security Capability Assessment was gathered using three discreet processes. Their findings equally contributed to the overall capability assessment analysis, maturity level assessment and the development of capability-building recommendations.

Extensive research was initially undertaken to analyse Cambodia's previous and current cyber security capability and knowledge states. This included researching past and recent cyber security incidents, legislation, and governance history to contextualise how Cambodian cyber security has developed over time.

Meetings and informal interviews were conducted via Microsoft Teams and Zoom with a range of Cambodian and Australian stakeholders within the public and private sector. Discussions were focussed on topics such as individuals' knowledge and skills relevant to cyber security, perspectives on Cambodia's cyber security maturity, and opinions on cyber security resources, education, and training accessibility.

Following interviews, a Cyber Security Capability Survey (the Survey) was designed using Survey Monkey to gather further quantitative and qualitative information about Cambodia's cyber security capabilities. The Survey was made up of 32 questions ([Appendix A](#)) designed to elicit information to fill gaps in current knowledge. The Survey was split into the five clusters outlined in [Section 4.1](#) (Cyber Security Governance and Standards, Capacity-building and Awareness, Legal and Regulatory, Cooperation, and Targeted Incident Response). Survey questions directly referred to the cluster's sub-section topics. This allowed maturity levels for each cluster and sub-section to be produced, providing an assessment of current cyber security capabilities and a metric to measure growth against in the future.

The Survey was distributed to senior stakeholders from MPTC, CADT, Ministry of Industry, Science, Technology and Innovation (MISTI), National Institute of Science, Technology and Innovation (NISTI) and the private sector, who were then asked to distribute the Survey to up to 80 people within their organisation for completion. Collectively, the Survey had capacity for 500 responses. Participants had six weeks to complete the Survey.

A total of 42 participants from MPTC and CADT completed the Survey. Due to limited participation, survey data was heavily skewed toward MPTC and CADT. Results of the Survey were analysed and are discussed in [Section 7](#).

6 Initial Findings

6.1 Documentation Review

Background

CyberCX conducted an open-source analysis of documentation on the history of Cambodia's cyber security and Cambodia's current cyber security capability. The open-source documentation review was comprised of documents that were released by the Cambodian Government, research institutes and international organisations.

Key themes

Cambodia is one of the fastest growing economies in the Indo-Pacific region, with economic activity being concentrated on the tourism, manufacturing and construction industries.⁴⁰ These industries have seen significant growth recently with the integration of digital technology into key infrastructure and an expanding focus on innovation.⁴¹ However, open-source documentation highlighted ongoing challenges for Cambodia in securing the integration of these new technologies.

The Cambodian ICT Masterplan defines a number of requirements, both financial and legislative, that will require support. It also defines a number of ICT systems and services that will require support. This places strain on Cambodia's limited budget. Budgetary constraints were subsequently identified as the greatest challenge to uplifting Cambodia's cyber security.⁴² Other blockers include the lack of essential, physical infrastructure and a skilled workforce shortage - including ICT security professionals, as well as those knowledgeable in cyber security, technical analysis, and human resources development.⁴³ Homeland defence and economic well-being are identified as the most critical factors negatively contributing to Cambodia's cyber security.⁴⁴

Research institutes highlighted that cyber-attacks in Cambodia are becoming increasingly sophisticated and difficult to detect and defend against.⁴⁵ Attack patterns demonstrate that DDoS and web defacement is most commonly used against Cambodia.⁴⁶ Other common attack vectors in Cambodia are phishing, SQL injection, email hijacking and telecom fraud.⁴⁷ The most targeted sites in Cambodia are Government websites, including websites of Ministries and Agencies, and the personal accounts of high-ranking Government officials.

The ASEAN Digital Masterplan 2025 provided an outline and roadmap to achieve planned regional cyber development objectives. The ASEAN Digital Masterplan strives toward a digitally enabled economy, focussing on security, sustainability, and transformation.⁴⁸ It articulates an ambition to innovate and integrate the ASEAN community, which includes the nations of Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam.⁴⁹

⁴⁰ 'Cambodia country brief', Department of Foreign Affairs. <https://www.dfat.gov.au/geo/cambodia/cambodia-country-brief>

⁴¹ 'The Science, Technology and Innovation Ecosystem of Cambodia', August 2021, United Nations Economic and Social Commission for Asia and the Pacific.

⁴² 'Summary on Cambodian ICT Masterplan 2020', 2014, KOICA.

⁴³ Mara Heng, and G. Hwang, October 2019, 'Analysis of Strategic Priorities for Strengthening Cyber Security Capability of Cambodia', Journal of Digital Convergence, vol. 17, no. 10: 93-102.

⁴⁴ Ibid.

⁴⁵ Ibid.

⁴⁶ Ibid.

⁴⁷ Nguon and Sun, January 2020, 'Cambodia v. Hackers'.

⁴⁸ 'ASEAN Digital Masterplan 2025', 2020.

⁴⁹ Ibid.

6.2 Key Themes from Stakeholder Interviews

Background

During this engagement, CyberCX conducted interviews with a diverse range of stakeholders on Cambodia's cyber security posture and capabilities. These stakeholders have included Cambodian subject matter experts from Australia, multilateral organisations in Cambodia, Cambodian Government officials and Cambodian cyber security subject matter experts.

A number of key themes were identified from these discussions.

Key themes

Low levels of cyber security awareness is a common issue in Southeast Asia, both at an individual and a nation-state level. Awareness is improving as nations increase their involvement with bilateral and multilateral partners such as Australia and ASEAN.

Mobile internet and data are easily accessible in Cambodia, supported by telecommunications providers in China, Vietnam, and Singapore. Cambodian citizens have increasingly turned to using the internet and social media as a medium for networking, connecting with others, working from home and as a source of news. High volumes of public messaging and media is run through social media platforms including Facebook, Telegram and Twitter. Commonly, individuals are reliant on mobile phones to utilise these platforms as their main or only internet connection. Internet cafes remain a connection method for a large proportion of internet users, which poses risks to individuals as these networks are susceptible to compromise through malware and viruses.

Non-government organisations and education groups exist in the region to enhance local communities' digital literacy. Disparity between younger and older generations in their vulnerability to cyber threats has been observed, with older individuals being at an elevated risk of compromise.

It is also common to see individuals and organisations in both private and public sector demonstrate a limited understanding of cyber security and the negative consequences of being compromised. Bring-your-own-device (BYOD) is very common in Cambodia, increasing the blurring between official systems and networks, and the broader internet.

Cybercrime is an issue which does not generate significant attention in Cambodian society. Additionally, access to cybercrime assistance is limited, with many not knowing where to go to report a cybercrime.

Mobile operators in Cambodia are described as having sufficient licencing and sim card quality.

Interviews highlighted workforce trends as a challenge, suggesting Cambodian citizens often do not seek careers in software engineering or ICT. This forces Cambodia to import ICT specialists from China, Singapore, and Malaysia. The highest skilled, sovereign IT specialists are commonly utilised in the military and in national security settings.

Regarding cyber security awareness within Cambodian society, Cambodians are aware of the advantages of cyber security at all levels of society and understand that data is used to run social, economic and political systems. It was highlighted that the Cambodian Government recognises the importance of developing technology in order to realise economic and social benefits. Local businesses also recognise the importance of having sufficient cyber security policies in place as part of a holistic and effective security posture. They understand the part cyber security plays in their economic success.

The greatest obstacle, however, is how to implement and achieve a contemporary and appropriate cyber security posture. Though people are aware of cyber security's positive implications,

implementation and execution of cyber security protections is overwhelming and difficult to begin. This is exacerbated by the lack of skilled workers available to support digital transformations.

Interviews identified variety in how organisations in Cambodia secure and fix their assets. Observations from private sector organisations suggest multinational companies have a lot of physical and logical protections over their IT systems and infrastructure. However, small-medium sized enterprises do not tend to have large, persistent systems. They typically prefer to run an IT system for a short period of time until it collapses or is compromised, at which point the system will be secured and stood back up. In comparison, when Government Agency websites are maliciously attacked and compromised, the website is often shut down and a new website is created as a replacement. Effort is not typically expended in securing the current asset.

7 Cyber Security Capability Analysis and Assessment

7.1 Cluster 1 - Cyber Security Governance and Standards

Cyber security governance and standards refers to an entity's ability to establish and enforce appropriate governance mechanisms and standards around cyber security, and its ability to consistently exercise good security practices. This includes considering whether organisations have cyber security action plans, crisis management documentation, opportunities to practice and test plans and adequate resources and tools to conduct cyber security planning and maintenance activities. Cyber defence and resilience are themes within this section, as well as building and strengthening national cyber security postures and trust in governments.

Cyber security governance has been identified by Cambodian stakeholders as an area for improvement due to many Government Ministries having limited or no roles and functions dedicated to cyber security.

This cluster includes the sub-sections:

- Baseline Security Measures
- Roles and Responsibilities

Cluster Snapshot:

Baseline Security Measures

Maturity Level

Early Definition →

5
4
3
2
1

Key Points

- Inconsistent implementation of baseline security requirements
- No Technology or BYOD Policy
- Limited staff understanding of baseline cyber security requirements

Next Step Objectives

1.2 Develop a cyber security baseline policy that describes standard security measures for all Cambodian Ministries

1.3 Conduct annual audits and ongoing regulatory checks of baseline security measures and high-risk assets

Roles and Responsibilities

Maturity Level

Early Definition →

5
4
3
2
1

Key Points

- It is difficult to recruit and retain qualified cyber security staff
- Staff balancing multiple roles have their cyber security responsibilities de-prioritised for other work

Next Step Objectives

1.1 Document roles and responsibilities for cyber internally and across Government

7.1.1 Establish Baseline Security Measures

Overview

Baseline security measures set a minimum-security benchmark for Government Ministries and the private sector to measure their cyber security posture and capabilities against. By setting a consistent cyber security standard across Government and the private sector, baseline security

measures also help encourage the use of common language between stakeholders, and provide guidance on how to prioritise their cyber security investments.

This sub-section considers the existence of baseline security measures across Government and how effectively current cyber security policy requirements are conveyed to and understood by Government staff.

Outcome

After consideration of the available evidence, the Cambodian Government was assessed as being *Maturity Level 2 – Early Definition* for its establishment of baseline security measures.

Detailed Results and Implications

Question 11 of the Survey ([Appendix A](#)) considered what security measures are already in place at Government Ministries. Of the 34 respondents, 14 provided the score 'Good', across an almost even distribution of MPTC and CADT staff. Most other respondents provided scores of 'Limited' and 'Average'. This suggests that uniform baseline cyber security requirements are still developing across both organisations, and that where measures are in place, they may still require maturation. Limited and/or inconsistent baseline security measures can threaten the security of Ministries as end-users and system infrastructure may be left vulnerable to malicious actors.

For organisations which have cyber security policies in place, Question 13 of the Survey ([Appendix A](#)) addressed how well individuals understand them. More than 50% of participants, both MPTC and CADT, indicated they had 'Limited Understanding'. This suggests respondents understand some of the requirements in the policies but not all of them (Figure 1). These insights show a breadth of understanding across both Ministries' staff, which indicates individuals are unlikely to be adhering to the policy requirements. Staff who are unaware of their organisation's cyber security policy and controls are more at risk of cyber-attack and may be engaging in activities that can create vulnerabilities in the organisation's security posture. Enforcing existing cyber security policies is an opportunity to accelerate achievement of baseline security measures.

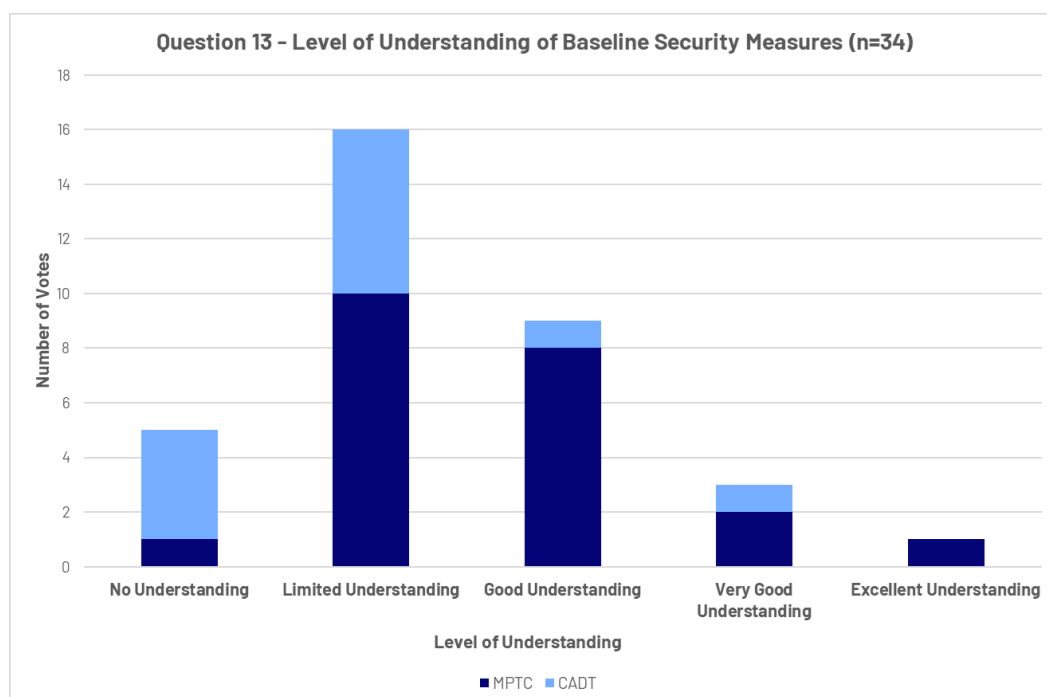


Figure 1 - Question 13 Survey Results

Insights from stakeholder interviews highlighted that technology shortages and staff skills gaps impact the Cambodian Government's ability to establish baseline security measures.

MPTC is currently developing regulations and frameworks to support baseline security measure implementation. This initiative is encouraging, however, low levels of Government technology utilisation may create challenges. MPTC noted staff members do not utilise Government distributed hardware and software, and instead will often use personal devices and email accounts for work purposes. It is difficult to apply consistent security controls across personal devices and ensure the patching of multiple different software products occurs. This increases the risk of devices and the Government information they hold being compromised.

Stakeholder interviews also recognised that MPTC is one of the key Ministries managing cyber security across the Cambodian Government. Despite this, MPTC does not have the capacity to support whole-of-Government cyber security posture uplift activities. Disparity in the cyber security baselines across Government Ministries poses a risk to the Cambodian Government's overall cyber security posture.

Recommendations

See recommended objectives in Section [8.1](#).

7.1.2 Roles and Responsibilities

Overview

Clearly defined roles and responsibilities play a critical role in cyber security management, reduction of risk, and the development of cyber security capability. This section considers the Cambodian Government's division of roles and responsibilities in its approach to cyber security, looking closely at what accountabilities exist, their effectiveness and how they can be strengthened.

Having clearly defined roles and responsibilities is important for planning, distribution of resources, and to support stakeholder understanding of their roles during a cyber security incident.

Outcome

After consideration of the available evidence, the Cambodian Government was assessed as being *Maturity Level 2 – Early Definition* for its definition of roles and responsibilities.

Detailed Results and Implications

The Survey identified that of the 23 MPTC respondents to Question 14 ([Appendix A](#)), just over half indicated that cyber security roles and responsibilities are '*Somewhat Defined*'. Five of the 11 CADT participants gave the same rating (Figure 2). The average score across both organisations suggests roles and responsibilities are determined only when an incident or crisis has been identified, rather than planned ahead of time. This means that MPTC and CADT may not be able to effectively respond to incidents, as suitably experienced and skilled resources may not be available when needed.

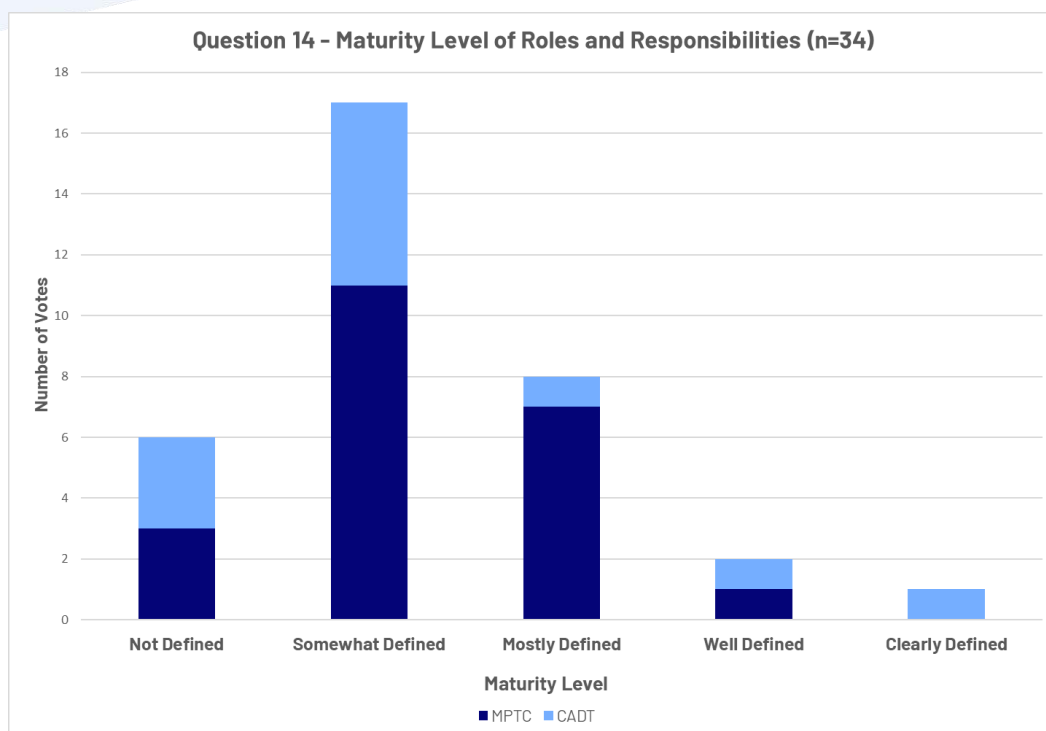


Figure 2 – Question 14 Survey Results

In stakeholder interviews, both MPTC and CADT noted the difficulty in recruiting a sufficient number of staff for open cyber security roles. Many staff held roles across multiple disciplines with differing sets of responsibilities. They were often forced to shift between areas such as digital forensics, malware analysis and higher priority incident response work. This demonstrates the high demand for cyber security staff and the challenges of deploying staff across functions, rather than having dedicated resources for each role.

Stakeholder interviews also noted that Ministries do not have a dedicated cyber security section. Instead, cyber security is fitted into a broader IT function. This results in people being placed into cyber security positions without sufficient knowledge or experience. These people are then unable to respond effectively to cyber threats when required. Similarly, stakeholder interviews highlighted that senior level stakeholders may not have technical or cyber security knowledge, meaning that there is limited top-down urgency behind cyber security activities, making it easy to de-prioritise.

The Cambodian Government is currently in the process of designing and establishing the Digital Security Committee and Digital Government Committee to facilitate and improve the Cambodian Government's digital transformation efforts. While stakeholders have noted that the lack of resources continues to be a challenge, they intend to continue the work. This ambition is positive for Cambodia's future cyber security approach.

Recommendations

See recommended objectives in Section [8.1](#).

7.2 Cluster 2 – Capacity-building and Awareness

This cluster will consider Cambodia's ability to raise awareness of and address cyber security risks and threats, as well as its ability to build and sustain cyber security capabilities over time.

Capacity-building is a broad target capturing a range of initiatives:

- Organising cyber security exercises
- Strengthening education and training programs
- Fostering research and development
- Developing incentives for private sector buy-in
- Increasing user awareness
- Establishing incident response capability

Collectively, improvements to these areas can contribute to overall uplift in skills and knowledge about the cyber security realm. This also supports assessment of Cambodia's ability to continuously build and improve cyber security capability in the future.

This cluster includes the sub-sections:

- Training and Education
- User Awareness
- Research and Development

Cluster Snapshot:

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

➡

5

4

3

2

1

Early Definition

7.2.1 Training and Education

Overview

Training and education programs are essential to enhancing cyber security operational capabilities in Cambodia. This sub-section analyses the Cambodian Government's provision of cyber security-specific training, focussing on the range of training available, alignment to international standards and accessibility for internal, private sector and public users.

Effective education and training programs that are aligned to international standards are an important foundational step in uplifting national cyber security capability.

Outcome

After consideration of the available evidence, the Cambodian Government was assessed as being *Maturity Level 2 – Early Definition* for training and education.

Detailed Results and Implications

Of the 30 survey participants who responded to Question 17 ([Appendix A](#)), the majority indicated that cyber security-specific training and education programs in Government are 'Average' or 'Limited' (Figure 3). This suggests Ministries do not provide cyber security-specific training to employees or only occasionally conduct cyber security-specific education, including awareness training. These insights show that there is opportunity for cyber security education and training to be developed and/or enhanced within Government Ministries, with increased frequency and expanded scope. Infrequent or ad hoc cyber security-specific training presents challenges to uplifting national cyber security capacity-building, as recipients of training may not be supported to regularly utilise or apply the skills they have learnt. Training should be conducted frequently to ensure knowledge retention and effective skills acquisition.

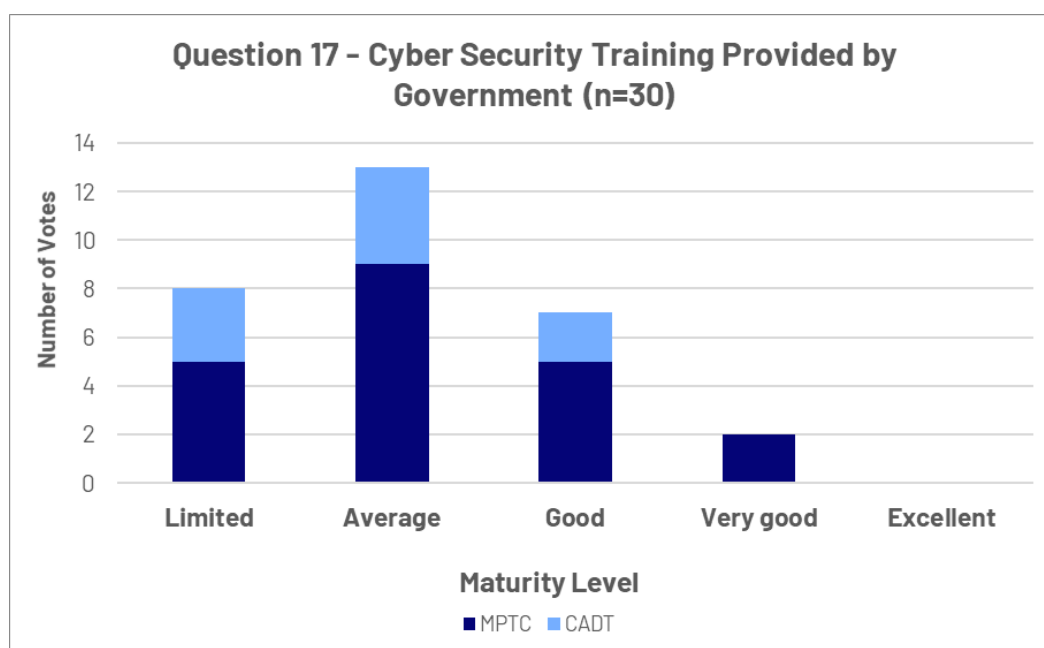


Figure 3 – Question 17 Survey Results

Survey insights showed alignment with insights gathered in stakeholder interviews. MPTC already conducts cyber security awareness training for staff and has good in-house capabilities, however due to various staffing limitations, skills are often not disseminated effectively and utilised after training. Similarly, MPTC had commenced conduct of training exercises for ICT leadership,

however, due to COVID-19 the training exercises were cancelled. This initiative indicates a maturing awareness of the importance of cyber security for senior and executive leadership.

While CADT has begun providing some cyber security training to Ministries, insufficient numbers of staff with cyber security knowledge has been a blocker to the expansion of the training program.

Stakeholder interviews highlighted training and education capabilities at inter-Ministry and international levels. At an inter-Ministry level, MPTC provides cyber security education and training resources to other Cambodian Government Ministries (detailed in Section 7.4.1). Due to shortages of resources capable of delivering cyber security training, training is infrequent and limited. The Cambodian Government is taking steps to mitigate this through engagement with international partners within the 'Train the Trainer' programs facilitated with partners including Japan and South Korea (detailed in Section 3.2). India also facilitates the provision of cyber security certifications to Cambodian Government employees through programs such as the IT Passport Program, intended to support development of the Cambodian Government's collective cyber skills and uplift the standard of cyber security knowledge.

During interviews, subject matter experts highlighted that in both Government and private sectors, individuals with technical skills often lack the soft skills needed to communicate to non-technical personnel. Education resources that pair soft skills with technical skills are still developing, but these plans highlight a sophisticated level of thinking and ambition regarding education and training. Lack of soft skills was identified in interviews as a key challenge for the Cambodian Government when developing cyber security policy, managing projects, and facilitating communication between relevant stakeholders. It was noted that this is not an issue unique to Cambodia, but a prominent challenge globally.

Recommendations

See recommended objectives in Section 8.2.

7.2.2 User Awareness

Overview

A whole-of-Government approach to improving user awareness is pivotal to uplifting Cambodia's cyber security posture. Ensuring end user security is crucial, as the end user is a common attack vector for malicious actors who use phishing and other social engineering techniques. This section analyses the level of cyber security user awareness possessed by Cambodian Government staff, and the effectiveness of the awareness training that is currently provided by the Government.

Outcome

After consideration of the available evidence, the Cambodian Government was assessed as being *Maturity Level 2 – Early Definition* for its levels of cyber security user awareness.

Detailed Results and Implications

Question 16 of the Survey asked participants to describe their overall cyber security awareness (Appendix A). All CADT participants responded either with 'Limited' or 'Average' awareness, while a significant majority of MPTC participants responded with 'Good', 'Very good' or 'Excellent' (Figure 4). Results from this question indicate a clear differentiation in cyber security awareness between Ministries, implying there is generally high cyber security awareness at MPTC in comparison to CADT. This suggests that MPTC may be nearing Maturity Level 3 for its user awareness capability.

It is important to note that those respondents from MPTC providing scores of 'Limited' or 'Average' identified themselves as working within executive and senior leadership positions, highlighting the importance of cyber security education and training for senior staff in Government Ministries. Senior staff who lack cyber security knowledge and awareness may pose a risk to Cambodian Ministries, as senior staff are commonly targeted by malicious actors through social engineering attacks.

MPTC leads the Cambodian Government's approach to cyber and provides cyber security awareness training to staff. The higher scores reflected in these findings support the effectiveness of previously delivered cyber security training.

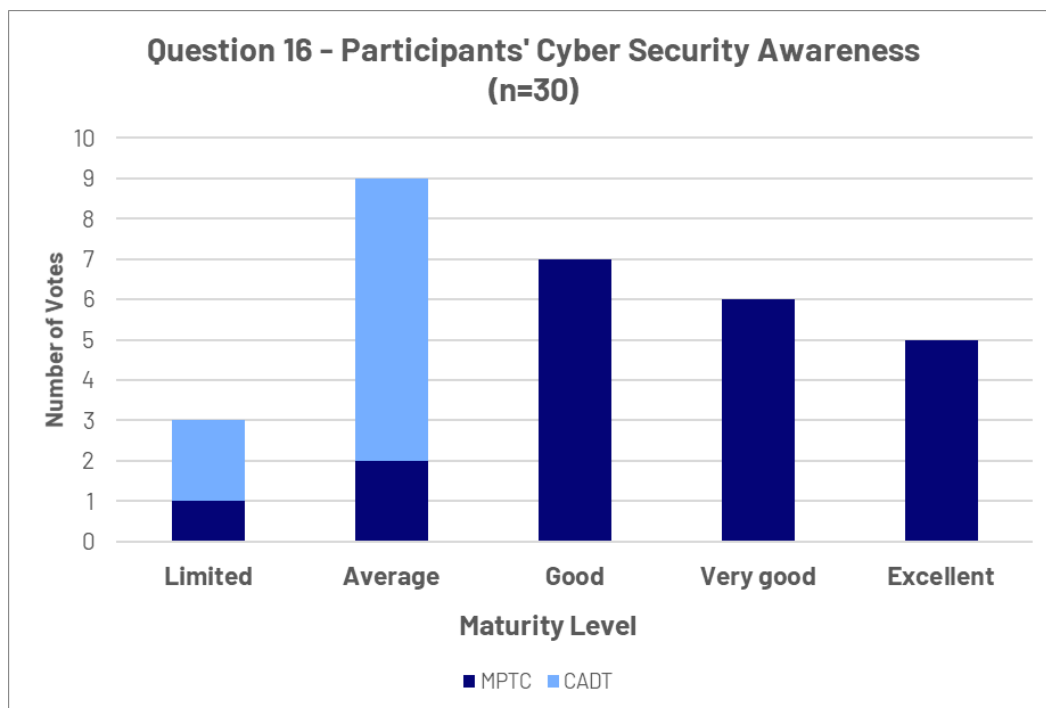


Figure 4 - Question 16 Survey Results

Public-facing cyber security awareness campaigns run by Government Ministries in Cambodia already exist, however, these were identified as 'Limited' or 'Average' or 'Good' by participants responding to Question 18 ([Appendix A](#)). No respondents provided a higher score than 'Good', suggesting that there are more opportunities to provide education to the general public on cyber security and its risks.

Insights from stakeholder interviews aligned with findings about awareness campaigns for the general public. Stakeholders described public cyber security awareness as a challenge due to cyber security language and jargon not directly or easily translating to Khmer. This creates a language barrier that prevents the easy dissemination of cyber security awareness information to the public. Stakeholders also noted members of the public often post personal and private information online through social media platforms without understanding the potential risks. MPTC also described its capacity to engage with the public as constrained due to limited resources with cyber security knowledge. CADT highlighted that it is in the process of developing a cyber training capability.

Stakeholder interviews also highlighted that recognition of the importance of cyber security is growing across the Cambodian Government. Consequentially, Government staff have a lot of questions about how they can better protect themselves. MPTC noted that the identification of phishing attacks can be challenging. Phishing attacks, especially those considered simple to

identify, is consuming a significant amount of MPTC's capacity. Phishing awareness training may help reduce the risks of individual users falling victim to a malicious phishing email, simultaneously reducing some of the burden on MPTC security teams.

The disparity in cyber security awareness and skills across the Cambodian Government presents a pertinent challenge to staff resourcing and the management of key issues. The uplift of public cyber security awareness also needs to be prioritised.

Recommendations

See recommended objectives in Section [8.2](#).

7.2.3 Research & Development

Overview

Research and development integrates the cyber security requirements of the Cambodian Government with the work of research groups to cultivate growth in cyber security capability and innovation. Fostering strong research and development initiatives provides the Cambodian Government with the foundations needed to identify priorities and develop capabilities suitable to meet the evolving threat landscape.

Outcome

After consideration of the available evidence, the Cambodian Government was assessed as being *Maturity Level 2 – Early Definition* for research and development.

Detailed Results and Implications

Of the 30 respondents to Question 19 ([Appendix A](#)), just over half indicated that their Ministry or organisation engaged in cyber security research and development 'Occasionally' (Figure 5). Qualitative information gathered in the Survey attempted to elicit further detail on what types of research, if any, had previously been conducted. Whilst minimal detail was provided, there was some evidence to suggest that MPTC has previously conducted at least one research project dedicated to cyber and that CADT is currently conducting a research and development project on cyber security in the private sector.

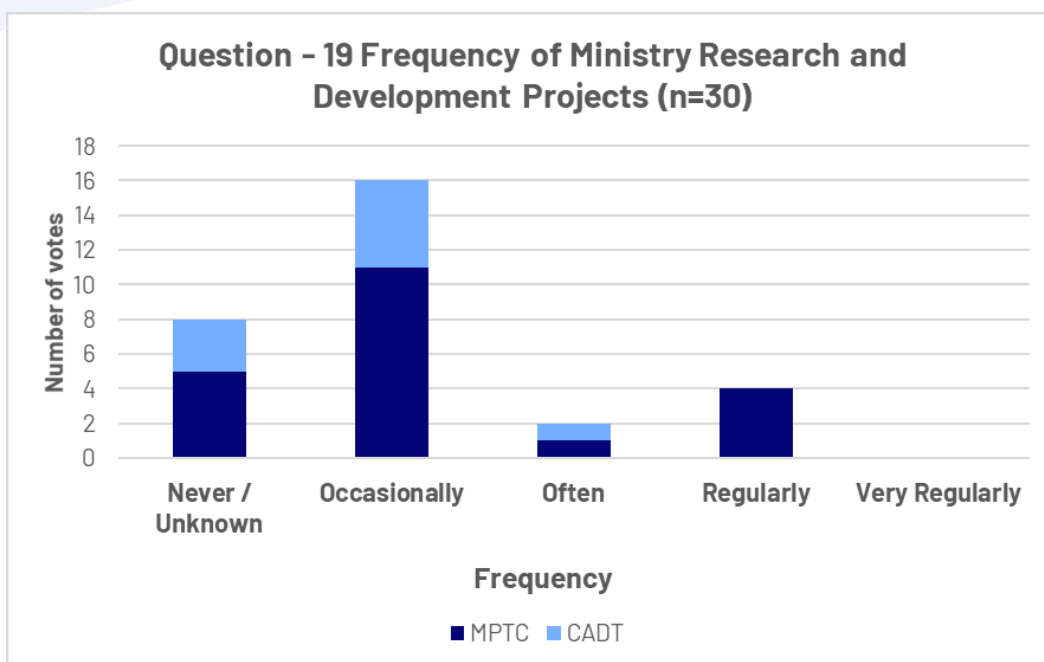


Figure 5 - Question 19 Survey Results

Insights from stakeholder interviews aligned with the information gathered in the Survey. MPTC described that it had previously conducted research and development projects focussed on cyber security capability and capacity-building. This was often restricted and constrained due to the ongoing challenge of limited staff resourcing and budget. CADT indicated that it has research capabilities for several differing subject areas, with a cyber security institution still in development.

Establishing a research and development capability and increasing the frequency and consistency of research and development projects would be beneficial for the Cambodian Government. This would assist in the development of a sovereign cyber security capability. Regular research and development would also support improved understanding of current and emerging cyber threats and landscapes, allowing time to develop mitigations prior to a security incident occurring.

Recommendations

See recommended objectives in Section [8.2](#).

7.3 Cluster 3 – Legal and Regulatory

This cluster analyses the Cambodian Government's capability and capacity to introduce and implement legal and regulatory measures to reduce cybercrime and malicious cyber incidents, and work toward protecting critical information infrastructure. There is also consideration for determining Cambodia's capability to develop a legal and regulatory framework designed to protect Cambodian citizens and businesses in the context of cyber security.

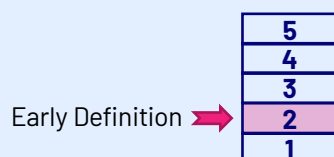
This cluster includes the sub-sections:

- Protection of Critical Information infrastructure
- Incident Reporting Framework

Cluster Snapshot:

Protection of Critical Information Infrastructure

Maturity Level



Key Points

- Some critical infrastructure operators are not aware of cyber security risks and do not invest in cyber security development

Next Step Objectives

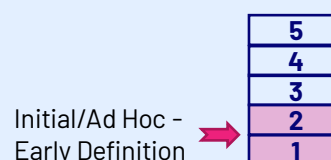
3.1 Formalise a list of Cambodian critical infrastructure operators and develop an engagement plan to address key cyber security topics and risks

3.2.1 Engage Ministries to support the development of cyber security legislation and maintenance

3.3 Update legislation to require Ministries to implement the minimum cyber security requirements developed in Objective 1.2 and encourage industry adoption

Incident Reporting Framework

Maturity Level



Key Points

- Sophistication of the current incident reporting hotline is limited
- Cyber security incident reporting resources are not well known and consistently accessible to the public and all Government staff. This reduces the ability of the public and Government staff members to report an incident when it occurs

Next Step Objectives

3.2.2 Strengthen methods for Ministries and the public to report cyber security incidents and crime

7.3.1 Protection of Critical Information Infrastructure

Overview

Critical information infrastructure encapsulates the technologies, devices, networks and ICT systems which are required for critical sectors, like power, energy, water, transport, financial services and telecommunications, to operate. This infrastructure is an increasingly attractive target for malicious cyber-attacks, making it important that Government commit to support and regulate its protection. Analysis described in this sub-section considers the current and future planned Government capabilities that will support and protect Cambodian critical information infrastructure.

Outcome

After consideration of the available evidence, the Cambodian Government was assessed as being *Maturity Level 2 – Early Definition* for its protection of critical information infrastructure.

Detailed Results and Implications

The majority of participants responded to Questions 21, 22 and 23 ([Appendix A](#)) with ‘*Limited*’ or ‘*Average*’, demonstrating that the prevalent view is that Ministries sometimes or do not at all identify and protect critical information infrastructure and digital service providers, and that Ministries sometimes or do not at all provide cyber security guidance and support to critical information infrastructure providers (Figure 6, Figure 7).

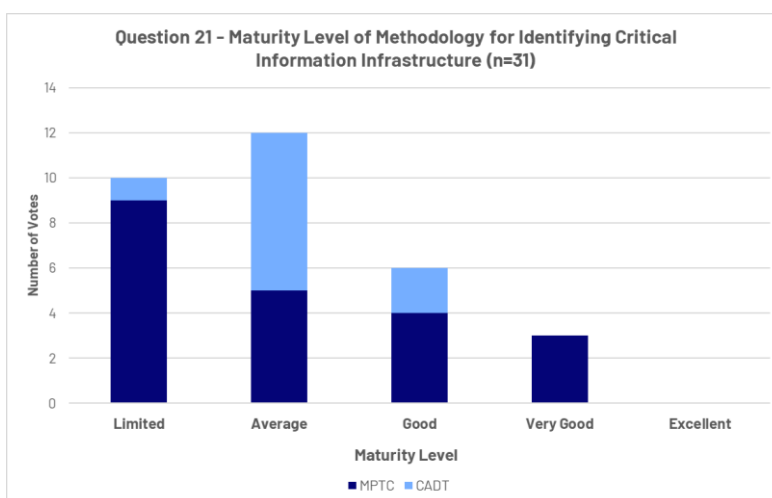


Figure 6 – Question 21 Survey Results

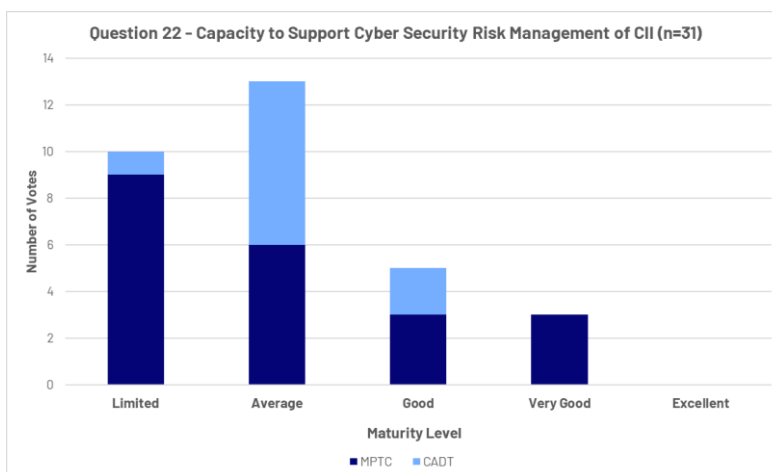


Figure 7 – Question 22 Survey Results

Ratings of ‘*Good*’ and ‘*Very Good*’ were received from participants within security teams in intermediate or leadership positions, suggesting that those with greater subject matter knowledge who work directly in this space may identify and engage more with critical infrastructure providers than other Ministry staff.

Stakeholder interviews revealed that MPTC has a list of critical information infrastructure and is undertaking a planning activity to better support these providers. Interviews provided additional insight into cyber security investment trends in Cambodia. Participants noted that the banking

and financial services industry currently invests heavily in cyber security, whereas critical infrastructure such as water suppliers and electricity, are not aware of relevant cyber threats. MPTC described continuous attempts over the last three years, to encourage critical infrastructure providers to invest in cyber security specialists within their teams. This is yet to be actioned. MPTC demonstrates awareness of cyber security's criticality for critical infrastructure providers, with stakeholders stating that more awareness and investment is required within provider organisations.

Recommendations

See recommended objectives in Section [8.3](#).

7.3.2 Incident Reporting Framework

Overview

Establishing effective incident reporting mechanisms is useful to gain understanding of the overall threat landscape, new and existing vulnerabilities and the impact a successful cyber-attack may have. Incident reporting platforms are also valuable for individuals who may have experienced cybercrime and require assistance of varying degrees. It is important that if a reporting platform exists, it is advertised and easily accessible.

Outcome

After consideration of the available evidence, the Cambodian Government was assessed as being *Maturity Levels 1-2 – Initial/Ad Hoc – Early Definition* for its current incident reporting framework capability.

Detailed Results and Implications

The majority of participants provided scores of 'Inaccessible' and 'Somewhat Accessible' in response to Questions 24 and 25 ([Appendix A](#)). These scores suggest reporting platforms are inaccessible or somewhat accessible with information sharing and reporting of cyber security incidents between Government and private sector being not effective or of limited effectiveness (Figure 8).

Higher scores were evident where participants worked within security teams in intermediate or leadership positions, suggesting that they may be more knowledgeable as to what resources are available and what information is shared between organisations, in comparison to other staff.

Stakeholder interviews provided limited insights into incident reporting frameworks, highlighting that a cybercrime hotline, which anyone can use to report an incident, is available in Cambodia. Though this suggests a reporting framework exists, enhancing its sophistication through further investment, and improving awareness of the resource will be necessary to uplift cyber security capability.

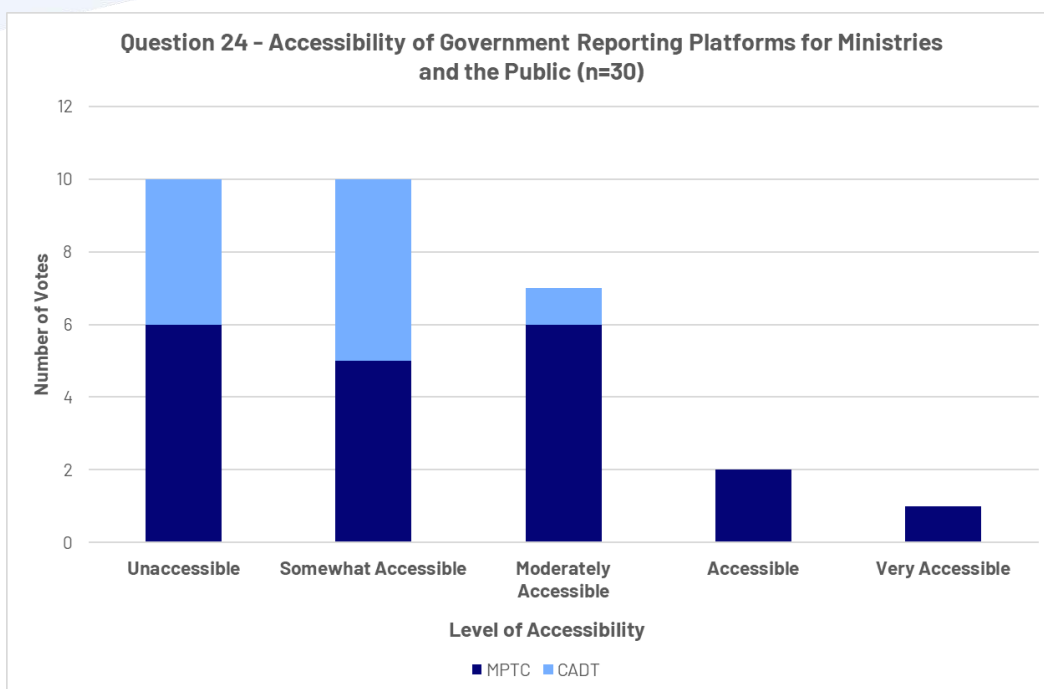


Figure 8 - Question 24 Survey Results

Recommendations

See recommended objectives in Section [8.3](#).

7.4 Cluster 4 – Cooperation

This cluster evaluates the cooperation and information sharing activities between stakeholder groups at the national and international level, to facilitate better understanding of and responses to the changing threat environment. National and international cooperation provides a platform to establish trusted partnerships, supporting growth and strategic development.

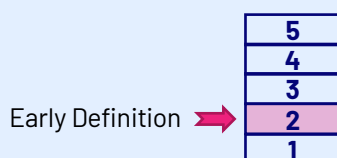
This cluster includes the sub-sections:

- Inter-Ministry Cooperation
- International Cooperation

Cluster Snapshot:

Inter-Ministry Cooperation

Maturity Level



Key Points

- Executive leadership, senior ICT and security staff provided higher self-assessed scores, indicating that greater knowledge correlates to roles that have greater involvement in inter-Ministry activities
- Inter-Ministry work to counter cybercrime is complex due to limited shared understanding of subject matter between stakeholders

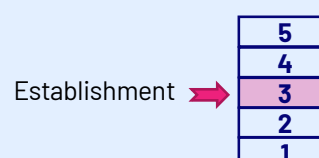
Next Step Objectives

4.1 Formalise a dedicated inter-Ministry committee and working groups to improve collaboration on cyber security topics

4.3 Develop national and international connections to foster greater cooperation on cyber issues and technology innovation

International Cooperation

Maturity Level



Key Points

- International cooperation already occurs between Cambodia and international partners
- The frequency of cooperation should continue to increase to facilitate and support Cambodia's cyber security capability development activities
- Cooperation should continue to be formalised to ensure that momentum and accountability can be maintained as growth occurs

Next Step Objectives

4.2 Strengthen international communication channels dedicated to discussing and sharing cyber security information

7.4.1 Inter-Ministry Cooperation

Overview

Cooperation between public agencies promotes support, collaboration, and capability alignment across Ministries and is encouraged by the Cambodian Government. A major benefit of inter-Ministry cooperation is that it helps reduce the risk of work being duplicated and ensures that limited cyber security resources are effectively deployed across Government. By cooperating and sharing competencies and resources, Ministries can work toward uplifting each other's cyber security capabilities without wasted effort.

Outcome

After consideration of the available evidence, the Cambodian Government was assessed as being *Maturity Levels 2 – Early Definition* for inter-Ministry cooperation.

Detailed Results and Implications

Of the 23 participants from MPTC and CADT who responded to Question 7 ([Appendix A](#)), over 50% indicated that the effectiveness of inter-Ministry communication channels when discussing cyber security were 'Not Effective/Unknown' or had 'Limited Effectiveness' (Figure 9). This suggests that there is limited formality in the engagement across Ministries on cyber security topics, meaning that information sharing may lack consistency and overall coherence. This inference is supported by responses to Question 8 ([Appendix A](#)), which demonstrates that Ministries meet to discuss cyber security and developments 'Occasionally', likely through informal communication channels only.

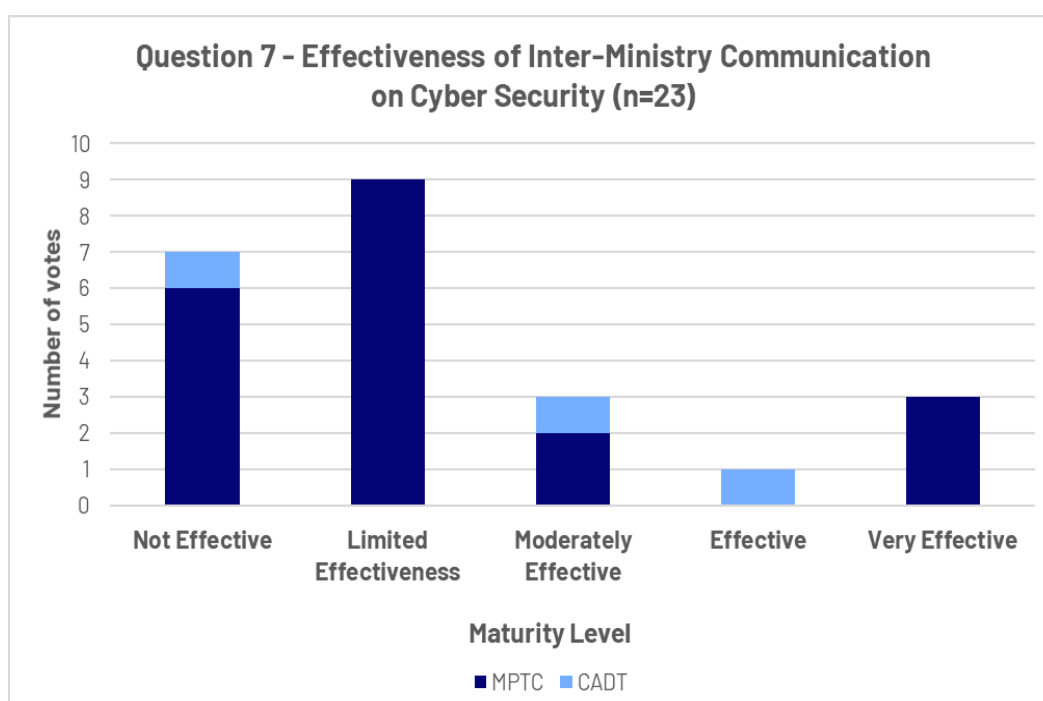


Figure 9 - Question 7 Survey Responses

Some participants from executive leadership, ICT senior and management, security, and financial teams provided scores of 'Effective' and 'Very Effective'. These scores characterise communication between Ministries dedicated to cyber security as being regular, formal and very effective.

CADT participants mostly provided scores of 'Moderately Effective' and 'Effective', indicating that communication occurs annually or twice annually, is moderately effective or effective, and that it takes place using established formal communication channels.

The breadth of scores indicates communication channels and processes may be in place, however, they are only known to or positively impact a small proportion of staff. This data demonstrates an opportunity for Ministries to strengthen these inter-Ministry communication channels and encourage their use among more teams.

Stakeholder interviews highlighted that MPTC provides education, training and support to other agencies in two ways. MPTC provides technical support and guidance to other Ministries, usually in the event of an incident. This aligns with higher scores from IT and security teams, as during an incident, these teams are likely to be those engaging in an inter-Ministry manner and will be highly connected to their counterparts in other Ministries. CADT then facilitates other education activities and provides support to other agencies. As a sub-section of MPTC, CADT provides training across Cambodian Government Departments and Agencies. This supports the higher scores provided by CADT respondents. These scores may also be influenced by the limited number of participants completing these questions in the Survey.

Other insights showed that inter-Ministry cooperation on countering cybercrime is complex, as there is a lack of shared understanding and knowledge across the different stakeholder groups involved in the investigation of cybercrime.

Recommendations

See recommended objectives in Section [8.4](#).

7.4.2 International Cooperation

Overview

Cooperation with Cambodia's international partners on cyber security is important to develop a common knowledge base and increase synergy between authorities on transnational crime. International cooperation also allows teaching and learning to occur between partners, contributing to each other's knowledge base and capability.

Outcome

After consideration of the available evidence, the Cambodian Government was assessed as being *Maturity Level 3 – Establishment* for its international cooperation.

Detailed Results and Implications

Of the 25 respondents to Question 9 ([Appendix A](#)), ten indicated that their Ministry engaged 'Effectively' with international partners on cyber security (Figure 10). Results from Question 10 ([Appendix A](#)), however, suggested that while effective, this engagement occurs only 'Occasionally'. These insights suggest Ministries engage effectively when meeting with international partners, however the frequency of these meetings could be increased to promote regular discussion on cyber security.

Stakeholder interviews identified a wide range of current engagement between international partners and Cambodian Ministries, specifically MPTC. Currently, MPTC acts as a facilitator when there is training or other support activities from another country, gathering other Ministries together to attend.

Several international partners have engaged with MPTC on cyber security capacity-building, including India, South Korea, Japan and Australia. For example, stakeholders from MPTC and CADT highlighted the partnerships with the South Korean and Japanese Governments on 'Train the Trainer' programs. The 'Train the Trainer' program is run through the Institute of Training at CADT in partnership with local academic institutes in partner countries. In addition, MPTC works closely with Indian IT companies to certify their digital skills and develop software and networks for the Cambodian Government.

These insights suggest there is appetite for international engagement and knowledge sharing. Based on these findings, it is evident that the frequency and quality of this knowledge sharing has an opportunity to grow and mature, promoting improved collaboration.

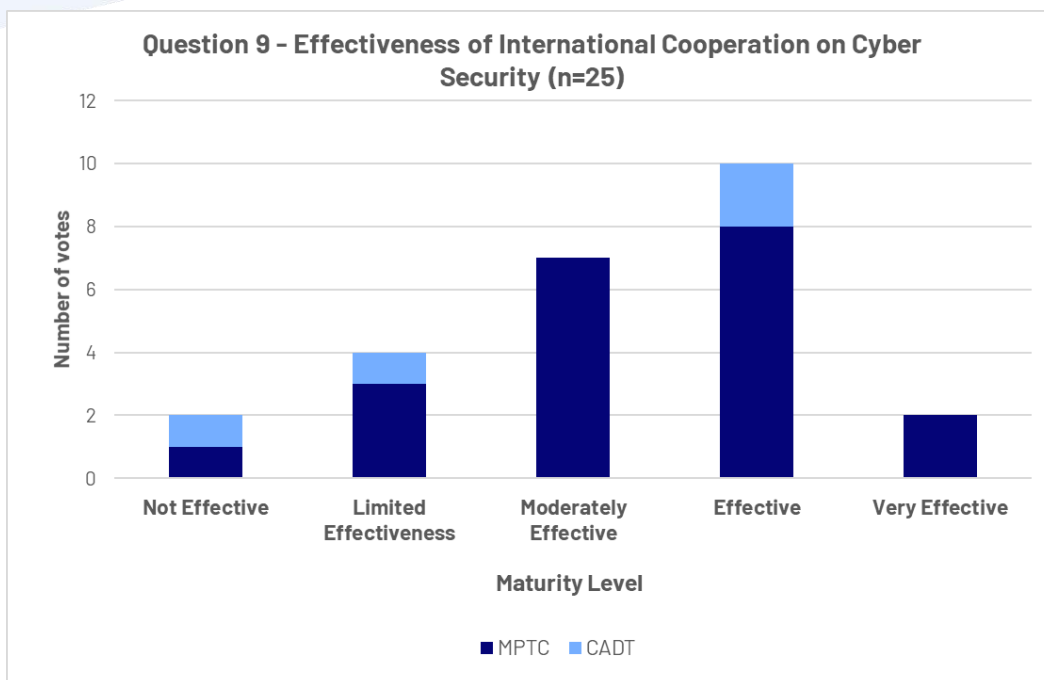


Figure 10 - Question 9 Survey Responses

Recommendations

See recommended objectives in Section [8.4](#).

7.5 Cluster 5 – Targeted Incident Response

This cluster considers Cambodia’s capacity and capability to respond to malicious cyber-attacks and incidents. Cambodian Government Ministries’ ability to respond effectively to cyber security incidents increases security defences, and decreases the potential risk of compromise, such as in ransomware deployments or acts of information espionage by malicious actors. Ineffective incident response may have serious consequences for the Cambodian Government and its national security. Therefore, uplifting this capability is vital for future Government protection. The Cambodian Government has already identified this as an area they would like to dedicate effort towards improving.

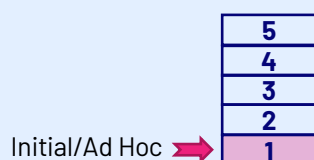
This cluster includes the sub-section:

- Operational Capabilities and Institutionalised Systems

Cluster Snapshot:

Operational Capabilities and Institutionalised Systems

Maturity Level



Key Points

- Ministries have limited confidence in their ability to successfully respond to a cyber security incident. They often do not have an incident response plan and even where one exists, it may not have been well publicised or tested
- Those responding to incidents are staffed across multiple roles, preventing them from specialising and further refining their specific cyber security skills

Next Step Objectives

5.0 Undertake cyber security incident response technical training

5.1 Develop and implement cyber security incident response plans for each Government Ministry and for whole-of-Government

5.2 Facilitate regular simulation exercises to test incident response skills in real-time conditions

5.3 Strengthen incident response resources, capability, and mechanisms across Ministries

7.5.1 Operational Capabilities and Institutionalised Systems

Overview

Strong incident response capabilities increase resilience against malicious cyber security attacks. Operational capabilities include the technical and operational elements required to support effective incident response. Enhancing workforce operational capabilities will contribute to uplifting the Cambodian Government’s incident response capability, its effectiveness and contribution to national security.

Outcome

After consideration of the available evidence, the Cambodian Government was assessed as being *Maturity Level 1 – Initial / Ad Hoc*. However, it is close to reaching Maturity Level 2 for operational incident response capabilities.

Detailed Results and Implications

Over 50% of survey participants provided the most limited scores ('No IR Plan', 'Never', and 'Immediately') for Questions 26, 28 and 29 (Appendix A), which relate to incident response operational capabilities (Figure 11, Figure 12, Figure 13). These scores correspond to participants never having been involved in a cyber security incident, organisations not having cyber security incident response plans, and, when a cyber security incident does occur, participants being likely to escalate managing the incident to another person immediately on discovering the signs of an incident.

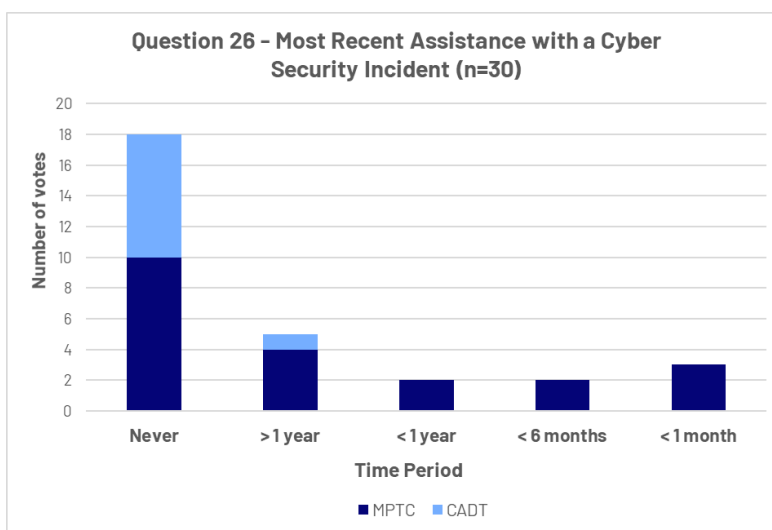


Figure 11 - Question 26 Survey Responses

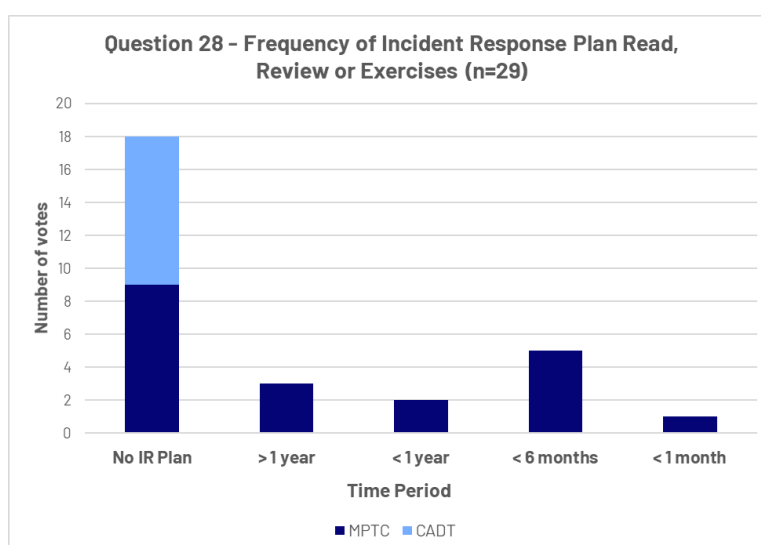


Figure 12 - Question 28 Survey Responses

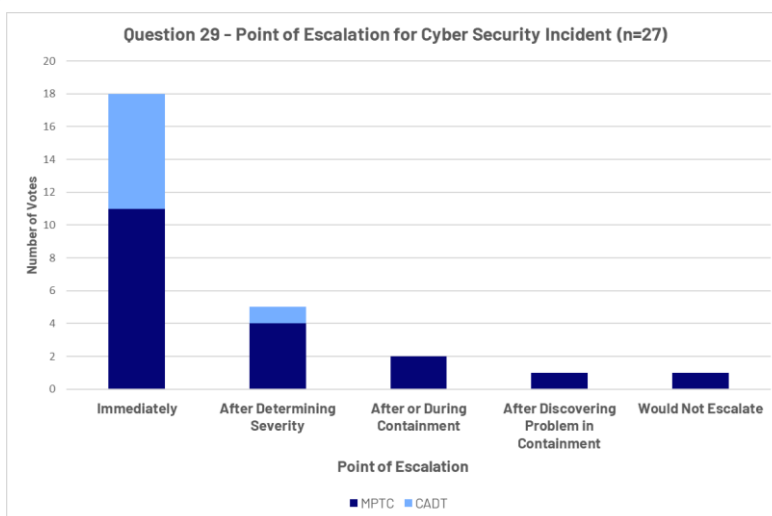


Figure 13 - Question 29 Survey Responses

Limited scores were provided by participants from ICT and security teams, non-technical teams, and leadership positions. This suggests knowledge gaps exist within teams responsible for responding to cyber security incidents, which poses a risk to the effectiveness of cyber security incident responses. This presents a positive opportunity for growth and learning.

In stakeholder interviews, MPTC responded that their digital forensics and incident response capabilities require improvement and face a range of challenges. MPTC has difficulty finding personnel skilled in incident response and only have a small team with limited capability who are familiar with the skills required. This restricts MPTC's ability to provide training to other Cambodian Government Ministries on the subject matter, despite often being asked to provide training, support, and assistance.

According to interviews, common incidents MPTC has been asked to respond to have included email spoofing, advanced persistent threat attacks and attacks on critical infrastructure. Currently, the Ministry does not have capability to undertake digital forensic investigations when an incident occurs. However, they are motivated to develop this capability. Open-source intelligence tools are mostly used for investigations and malware analysis. Members of MPTC are trained to conduct malware analysis activities alongside incident investigation, however, due to their lack of resources, malware analysis is often deprioritised in favour of incident response. MPTC is looking to develop malware analysis capacity across the Cambodian Government to provide each Ministry with the capability to undertake its own malware analysis activities.

MPTC intends to transition to online digital systems for monitoring and investigating incidents.

Details on cyber security incidents in the Cambodian Government are not publicly disclosed. At time of writing, no information on how these attacks occur was found.

Recommendations

See recommended objectives in Section [8.5](#).

8 Future Capability and Roadmap

Based on the evidence gathered in this Cyber Security Capability Assessment, several enhancement objectives have been identified. These have been designed to contribute to uplifting Cambodia's cyber security resilience and capability. Objectives have been separated into short-, medium- and long-term goals, with some achievable in Phase 2 of this project (Figure 14).

	Phase 2	Short-Term	Medium-Term	Long-Term
1. Governance and Standards		1.1 Document roles and responsibilities for cyber internally and across Government	1.2 Develop a cyber security baseline policy that describes standard security measures for all Cambodian Ministries	1.3 Conduct annual audits and ongoing regulatory checks of baseline security measures and high-risk assets
2. Capacity-building and Awareness	2.0 Conduct a cyber security awareness program delivered to selected Cambodian Government staff and Trainers	2.1.1 Implement a phishing email simulation tool to complement the cyber security awareness program 2.1.2 Engage with executive and senior leadership for cyber security awareness training and alignment of cyber security requirements within policy	2.2 Promote public awareness of cyber security and the importance of understanding cyber security issues	2.3 Develop a cyber security research and development strategy to strengthen cyber research and development activities
3. Legal and Regulatory		3.1 Formalise a list of Cambodian critical infrastructure operators and develop an engagement plan to address key cyber security topics and risks	3.2.1 Engage Ministries to support the development of cyber security legislation and maintenance 3.2.2 Strengthen methods for Ministries and the public to report cyber security incidents and crime	3.3 Update legislation to require Ministries to implement the minimum cyber security requirements developed in Objective 1.2 and encourage industry adoption
4. Cooperation		4.1 Formalise a dedicated Inter-Ministry committee and working groups to improve collaboration on cyber security topics	4.2 Strengthen international communication channels dedicated to discussing and sharing cyber security information	4.3 Develop national and international connections to foster greater cooperation on cyber issues and technology innovation
5. Targeted Incident Response	5.0 Undertake cyber security incident response technical training	5.1 Develop and implement cyber security incident response plans for each Government Ministry and for whole-of-Government	5.2 Facilitate regular simulation exercises to test incident response skills in real-time conditions	5.3 Strengthen incident response resources, capability, and mechanisms across Ministries

Figure 14 - Cyber Security Resilience Roadmap

Each objective is described in detail from pages 41 to 52.

8.1 Cyber Security Governance and Standards

The following recommended objectives relate to the Cyber Security Governance and Standards cluster.

Objective 1.1: *Document roles and responsibilities for cyber internally and across Government*

Priority: Short-term

Description:

- a) Define cyber security roles to align with the cyber security responsibilities in MPTC. This should encompass the following functions:
 - i. Cyber security governance
 - ii. Regulatory overviews
 - iii. Ongoing monitoring
 - iv. Cyber security solution design
- b) Document roles and responsibilities for cyber across Government, including performance expectations. This may include:
 - i. Developing legislation
 - ii. Investigating cybercrime
 - iii. Developing cyber policy
 - iv. Servicing IT systems
 - v. Coordinating and planning engagement with international partners
 - vi. Responding to cyber security incidents
 - vii. Providing cyber security advice and resources to the public and industry

Target Audience: Whole-of-Government

Intended Outcome and Value: To develop consistent understanding of cyber security roles and responsibilities across Government. This will ensure that Government stakeholders understand where responsibilities for cyber security sit and will support the appropriate resourcing of key capabilities.

Justification: Stakeholder interviews and data from the Survey indicated that roles and responsibilities relating to cyber security are not clearly defined. Those in cyber security roles commonly have several sets of responsibilities across different roles, creating difficulties in appropriately prioritising cyber security work.

Objective 1.2: *Develop a cyber security baseline policy that describes standard security measures for all Cambodian Ministries*

Priority: Medium-term

Description:

- a) List minimum cyber security requirements for all Cambodian Ministries and organisations to align with. These may include:
 - i. Regular information backups
 - ii. Antivirus protection
 - iii. Password requirements
 - iv. Multi-factor authentication
 - v. Risk management
 - vi. BYOD policy

Target Audience: Whole-of-Government

Intended Outcome and Value: To establish mature cyber security standards across Government, uplifting the overall security of Ministries' staff by reducing preventable cyber vulnerabilities.

Justification: Stakeholder interviews and data from the Survey indicated that no standard technology or BYOD policies are enforced in Ministries. Where baseline cyber security standards are evident, inconsistencies in how standards are applied exist between Ministries.

-
- b) Conduct capacity-building exercises to build self-sufficient capability in each Ministry, ensuring consistent understanding of cyber security policy baselines and enabling compliance with defined requirements
 - c) Review the cyber security baseline policy annually to ensure requirements remain current and relevant

Objective 1.3: *Conduct annual audits and ongoing regulatory checks of baseline security measures and high-risk assets*

Priority: Long-term

Description:

- a) Conduct annual compliance audits and checks to ensure that Ministries are meeting the baseline cyber security requirements set under Objective 1.2
- b) Conduct annual compliance audits of high-risk assets to ensure they are compliant with baseline cyber security standards. High-risk assets may include:
 - i. Critical infrastructure
 - ii. Information repositories
 - iii. Web servers

Target Audience: Whole-of-Government

Intended Outcome and Value: To ensure that assets meet minimum cyber security requirements, reducing preventable vulnerabilities. Regular audits should ensure that visibility over Government ICT portfolios is maintained, including where further work will be required to meet defined security standards.

Justification: Stakeholder interviews and data from the Survey indicated no long-term auditing currently occurs to ensure cyber security measures are enforced. Timely audits and reviews will help ensure that defined cyber security standards are being met by all Government Ministries, providing a consistent baseline for Cambodian organisations.

8.2 Capacity-building and Awareness

Objective 2.0: *Conduct a cyber security awareness program delivered to selected Cambodian Government staff and Trainers*

Priority: Phase 2

Description:

- a) Provide cyber security awareness training to selected Cambodian Government staff and Trainers. CyberCX will provide cyber security awareness training during a week-long period in Cambodia, along with training material to support Cambodian Trainers to roll the training out to the whole-of-Government.
- b) Training may include:
 - i. Suspicious or malicious links
 - ii. Password security
 - iii. Digital footprint awareness
 - iv. Online identity risks and mitigations

Target Audience: Selected individuals and Trainers to provide the capability to roll out to the whole-of-Government.

Intended Outcome and Value: To support cyber security awareness uplift across the Cambodian Government. Staff will be better able to recognise malicious cyber activities and will be more effective at protecting themselves online.

Justification: Stakeholder interviews and data from the Survey indicated that staff at all levels (junior to executive) have limited understanding of and confidence in foundational cyber security knowledge and how to apply it.

Objective 2.1.1: *Implement a phishing email simulation tool to complement the cyber security awareness program*

Priority: Short-term

Description:

- a) Implement a phishing email simulation tool across whole-of-Government to complement the cyber security awareness program
- b) The tool should provide foundational education on how to identify and report phishing emails and potentially malicious social engineering attempts, generate and distribute periodic phishing emails to Cambodian Government staff and provide reports on the rate of identification/reporting.

Target Audience: Whole-of-Government

Intended Outcome and Value: To reinforce lessons learned in the cyber security awareness program and educate staff to identify phishing emails. Staff will be better able to recognise malicious cyber activities and will be more effective at protecting themselves online.

Justification: Stakeholder interviews and data from the Survey indicated that staff at all levels (junior to executive) have limited understanding of and confidence in foundational cyber security knowledge and how to apply it.

Objective 2.1.2: *Engage with executive and senior leadership for cyber security awareness training and alignment of cyber security requirements within policy*

Priority: Short-term

Description:

- c) Conduct cyber security awareness training for all executive and senior leadership staff that do not have technical backgrounds. This should include training on cyber security risks and their mitigations
- d) Analyse how the connection between cyber security policy and technical capability in the Cambodian Government can be strengthened and identify remediation activities

Target Audience: Executive and senior leadership Government staff

Intended Outcome and Value: To build senior leadership awareness of cyber security risks and the current threat landscape. Improved awareness at a senior level will be critical to the success of other planned cyber improvement activities.

Justification: Stakeholder interviews and data from the Survey indicated that multiple senior staff members lack general cyber security awareness, meaning that they may not be able to recognise malicious social engineering attempts. As senior staff are attractive targets for malicious actors, their ability to recognise and report such attempts is vital for the overall protection of their Ministry or organisation.

Objective 2.2: *Promote public awareness of cyber security and the importance of understanding cyber security issues*

Priority: Medium-term

Description:

- a) Engage with the public through media campaigns to highlight the importance of staying secure online
- b) Facilitate campaigns utilising popular platforms in Cambodia including:
 - i. Facebook
 - ii. WhatsApp
 - iii. Telegram
- c) Provide free online resources for the Cambodian public, including:
 - i. Guides on staying secure online
 - ii. Guides on what to do if you are the victim of a cyber-attack
 - iii. Case studies on recent malicious campaigns and scams

Target Audience: Cambodian public

Intended Outcome and Value: To build cyber security awareness and resilience by uplifting cyber security comprehension across the Cambodian population.

Justification: Stakeholder interviews and data from the Survey indicated that awareness campaigns for the public are not regularly conducted in Cambodia. The language barrier was noted as being a significant challenge, as security content must be translated into Khmer to be understood by the broader Cambodian population.

Objective 2.3: *Develop a cyber security research and development strategy to strengthen cyber research and development activities*

Priority: Long-term

Description:

- a) Develop a cyber security research and development strategy. Research and development activities may include:
 - i. Providing grants to grow the cyber security industry
 - ii. Developing partnerships with universities
 - iii. Planning to grow education and skills pipelines to decrease workforce shortages

Target Audience: Government and private industry including universities and research facilities

Intended Outcome and Value: To foster growth in the local cyber security market by increasing sovereign capabilities and intellectual property. This will support job creation and market growth, improving the availability of skilled cyber security professionals in Cambodia.

Justification: Stakeholder interviews and data from the Survey indicated that a very limited number of research and development activities had been established to address cyber security concerns.

8.3 Legal and Regulatory

Objective 3.1: *Formalise a list of Cambodian critical infrastructure operators and develop an engagement plan to address key cyber security topics and risks*

Priority: Short-term

Description:

- a) Formalise definition of critical infrastructure in Cambodia
- b) Develop a list of critical infrastructure providers in Cambodia
- c) Approach critical infrastructure providers to understand their current cyber security capabilities and where engagement with Government will be most effective

Target Audience: Cambodian Government and critical infrastructure service providers

Intended Outcome and Value: To understand what critical infrastructure providers exist and the current state of their cyber security capabilities. This will assist in determining how the Cambodian Government can best support cyber security uplift requirements across critical infrastructure.

Justification: Critical infrastructure (powerplants, telecommunications providers, water, and financial facilities) is a common target for malicious cyber actors. Stakeholder interviews and data from the Survey indicated that limited support is currently provided by Government to these entities to assist them in defending against cyber security threats.

Objective 3.2.1: *Engage across Ministries to support the development of cyber security legislation and maintenance*

Priority: Medium-term

Description:

- a) Seek feedback from across Ministries on current cyber security legislation
- b) Collaborate to fill gaps in current legislation
- c) Engage with private industry to ensure legislation includes private sector considerations

Target Audience: Legislation development teams in Government

Intended Outcome and Value: To collaboratively develop legislative improvements and new legislation which encapsulates Ministry and private sector needs and cyber security requirements.

Justification: Stakeholder interviews and data from the Survey indicated that legislation dedicated to cyber security is limited and that its development is not usually the product of inter-Ministry collaboration.

Objective 3.2.2: *Strengthen methods for Ministries and the public to report cyber security incidents and crime*

Priority: Medium-term

Description:

- a) Uplift accessibility and functionality of incident reporting platforms and mechanisms for the public and Ministries
- b) Market the reporting platforms to improve awareness of their existence
- c) Report findings to Government annually, including the number of reported cyber security incidents and whether they were addressed and/or resolved
- d) Pass relevant incidents and/or information about cyber-attacks on to police for investigation

Target Audience: Whole-of-Government and the Cambodian public

Intended Outcome and Value: To provide support to individuals who may have been compromised, impacted by a cyber-attack, or otherwise been made the victim of cybercrime. Recording metrics across the reports received creates visibility for the Cambodian Government and police over how much cybercrime occurs, the key types of cybercrime, and what resources are needed to effectively protect against it.

Justification: Stakeholder interviews and data from the Survey indicated that though a cyber security incident hotline exists, it is not well-known, and its purpose is not clearly understood. There is no separation in reporting methods for Government staff and the public.

Objective 3.3: *Update legislation to require Ministries to implement the minimum cyber security requirements developed in Objective 1.2 and encourage industry adoption*

Priority: Long-term

Description:

- a) Consider all minimum cyber security requirements intended to be enforced across all Ministries
- b) Update legislation to reflect the enforcement of minimum cyber security requirements
- c) Engage with private sector to promote the adoption of these requirements in industry

Target Audience: Whole-of-Government and the private sector

Intended Outcome and Value: To establish enforceable minimum cyber security standards across all Ministries, contributing to an uplift in maturity and resilience across industry and the whole-of-Government.

Justification: Stakeholder interviews and data from the Survey indicated that no minimum cyber security requirements for Government Ministries or private sector exist. Varying levels of cyber security maturity and inconsistent practices are evident across Ministries.

8.4 Cooperation

Objective 4.1: *Formalise a dedicated inter-Ministry committee and working groups to improve collaboration on cyber security topics*

Priority: Short-term

Description:

- a) Establish an inter-Ministry cyber security committee to govern national and international collaboration opportunities on cyber security, ensuring appropriate representation of each Ministry
- b) Create cyber security working groups within each Ministry to support discussion of cyber security topics and maintain visibility within each Ministry. Cyber security working groups would report to the inter-Ministry cyber security committee
- c) Utilise the inter-Ministry committee to support collaboration on:
 - i. Cyber security policy
 - ii. Incident identification and response
 - iii. Baseline security measures

Target Audience: Whole-of-Government

Intended Outcome and Value: To uplift cooperation and collaboration on cyber security, encouraging the sharing of cyber intelligence and specialist skills. Working groups within Ministries may also act as a cyber security advisors for their respective Ministries and should be able to hold people accountable for non-compliance with minimum cyber security requirements.

Justification: Stakeholder interviews and data from the Survey indicated that there is a lack of cyber security collaboration and subject matter governance within and across Cambodian Ministries. Ministries have varying levels of cyber security awareness and are inconsistent in how they talk about and act on cyber security matters.

Objective 4.2: *Strengthen international communication channels dedicated to discussing and sharing cyber security information*

Priority: Medium-term

Description:

- a) Establish dedicated cyber security communication and collaboration channels between Ministries and international partners. This should be facilitated and governed by the cyber security committee established under Objective 4.1. Collaboration opportunities may encompass:
 - i. Information sharing with regional partners at multilateral forums
 - ii. Collaboration on international cyber security initiatives
 - iii. Coordination with ASEAN to uplift regional cyber security maturity

Target Audience: Cambodian Government and international partners

Intended Outcome and Value: To ease communication and collaboration on cyber security between the Cambodian Government and international partners, promoting regional cyber security resilience, support, and innovation.

Justification: Stakeholder interviews and data from the Survey indicated cooperation between Cambodia and international partners occurs. However, time is not always dedicated to cyber security and cooperation does not always occur formally. Communication channels dedicated to discussing cyber security do not exist.

-
- iv. Aligning cyber security uplift within Cambodia with international initiatives such as the ASEAN Digital Masterplan
-

Objective 4.3: *Develop national and international connections to foster greater cooperation on cyber issues and technology innovation*

Priority: Long-term

Description:

- a) Develop national and international connections to strengthen bilateral relationships developed under Objective 4.2
- b) Mature new and existing relationships by raising cyber security issues at national and international meetings, summits and conferences to promote the importance of cyber security

Target Audience: Cambodian Government, international and national partners

Outcome and Value: To mature relationships with national and international partners and strengthen strategic discussion around cyber security.

Justification: Stakeholder interviews and data from the Survey indicated that cyber security engagement between Cambodia and international partners does occur but is not yet mature in nature and does not fully consider regional and strategic level discussion points.

8.5 Targeted Incident Response

Objective 5.0: *Undertake cyber security incident response technical training*

Priority: Phase 2

Description:

- a) CyberCX to facilitate introductory Triage cyber security incident response training for a targeted group at MPTC to uplift capability. This will focus on:
 - i. Incident response process
 - ii. Roles and responsibilities
 - iii. Incident triaging
 - iv. Basic triage forensics
 - v. Escalation processes
- b) CyberCX to encourage the initial group to disseminate their learnings to other Ministries to assist in building in-house capability across the Cambodian Government

Target Audience: MPTC cyber security team

Outcome and Value: To uplift incident response technical experience, knowledge, and capability within MPTC.

Justification: Stakeholder interviews and data from the Survey indicated that teams within MPTC and CADT lack confidence and experience with responding to cyber security incidents. They may not be able to effectively respond to cyber security incidents affecting Government when required.

Objective 5.1: *Develop and implement cyber security incident response plans for each Government Ministry and for whole-of-Government*

Priority: Short-term

Description:

If a cyber security incident response plan does not already exist:

- a) Host an initial workshop to understand key Ministry requirements
- b) Based on discussion, develop a cyber security incident response plan detailing the steps required to successfully detect, investigate, triage and resolve a cyber security incident

If a cyber security incident response plan does already exist:

- c) Conduct an initial review of the existing incident response plan
- d) Host a workshop to understand gaps in the existing plan
- e) Uplift the existing plan based on improvements discussed in the workshop

Target Audience: Whole-of-Government

Outcome and Value: To build preparedness, confidence, and formalisation of the cyber security incident response process, so that when required, cyber security incident responses can be effectively deployed.

Justification: Stakeholder interviews and data from the Survey indicated that staff working in relevant cyber security roles do not know of existing cyber security incident response plans.

Objective 5.2: *Facilitate regular simulation exercises to test incident response skills in real-time conditions*

Priority: Medium-term

Description:

- a) Conduct regular, mock cyber security incident response exercises for teams who are involved in responding to cyber security incidents within each Ministry and at the inter-Ministry level
- b) Document and present findings from exercises to executive leadership to promote understanding of the threat landscape and promote the need for resourcing and investment in cyber security

Target Audience: Government cyber security teams

Outcome and Value: To support cyber security teams by providing the learning and practice required to improve their cyber security incident response skills. Individuals should be able to build specialised skills and confidence in the use of incident response tools, building resilience and preparedness for when a real incident occurs.

Justification: Stakeholder interviews and data from the Survey indicate testing of incident response plans does not currently occur within MPTC or CADT, allowing no time for staff to practice and refine their technical skills.

Objective 5.3: *Strengthen incident response resources, capability, and mechanisms across Ministries*

Priority: Long-term

Description:

- a) Collect and collate reports on cyber security incidents, documenting trends and patterns of threat actor behaviour
- b) Share lessons learned across Ministries, utilising the Ministry working groups and the committee established under Objective 4.1
- c) Upskill Ministry staff who may have a desire re-train and support them to join the cyber security teams performing incident response activities
- d) Develop threat intelligence to support ongoing understanding of the current threat landscape. This will allow the Cambodian Government to prepare for likely attacks before they occur

Target Audience: Whole-of-Government

Outcome and Value: To continue uplifting cyber security incident response capabilities and resources across Government over time.

Justification: Stakeholder interviews and data from the Survey indicated that current incident response capability lacks maturity, as the limited pool of skilled resources has constrained availability due to demand for individuals' skills across other, higher-prioritised work.

9 About CyberCX

Australia's greatest force of cyber security experts.

The CyberCX group brings together the country's most trusted cyber security companies to create a comprehensive end-to-end cyber security service offering to Australian enterprise and government.

With a workforce of over 950 cyber security professionals, and a footprint of over 20 offices across Australia and New Zealand, and global presence in Europe and the US, CyberCX offers a full suite of cyber security services.

Our expertise is represented across 12 cyber security practices:

- Strategy & Consulting
- Security Testing & Assurance
- Governance, Risk & Compliance
- Security Integration & Engineering
- Identity & Access Management
- Secure Digital Transformation
- Managed Security Services
- Digital Forensics & Incident Response
- Cyber Capability, Education and Training
- Privacy Advisory
- Cyber Intelligence
- Training & Education

Led by industry experts and delivered by cyber security specialists committed to their craft, CyberCX represents Australia's best cyber security talent, applying unmatched cyber security expertise to protect and defend Australian organisations from cyber threats.

10 Appendices

Appendix A Cyber Security Capability Survey Questions

Personal Information						
Question		Answer Options				
1	Which age range are you in?	18-25	26-35	36-50	51+	
2	How many years of experience do you have in your current industry?	Less than 1 year	1-5 years	6-10 years	11-15 years	16+ years
3	Which Ministry or organization do you work at? (If multiple options apply, select the most specific one)	CamCERT	MISTI	NISTI	MPTC	CADT
		Another Ministry	An education institution	A research institute	A private enterprise	
4	What division of this organization are you in?	Education team	ICT team	Policy team	Security team	Leadership
		Other (please specify)				
5	How long have you worked at your current organization?	0-6 months	7-12 months	1-5 years	6-10 years	11+ years
6	Which of these best describes the seniority of your role?	Entry level	Intermediate	Senior	Manager	Executive
Governmental Cyber Security Cooperation						
Question		Answer Options				
7	How effective are the communication channels with other ministries when discussing cyber security?	Not effective / Unknown - Communication between Government Ministries on cyber	Limited effectiveness - Communication between Government Ministries on cyber security occurs	Moderately effective - Communication between Government Ministries on cyber security occurs	Effective - Communication between Government Ministries on cyber security occurs	Very effective - Communication between Government Ministries on cyber security occurs

		security does not occur	through informal communication channels or infrequent/rare meeting groups for inter-Ministry discussions on cyber security.	through formal communication channels or regular meeting groups for inter-Ministry discussions on cyber security.	through formal communication channels used frequently for inter-Ministry communication on cyber security. Regular meetings occur to discuss cyber security. An emergency communication channel exists and is sometimes exercised.	through formal communication channels dedicated to cyber security with uniform information requirements. Regular meetings occur and are dedicated to discussing cyber security. An emergency communication channel exists and is exercised frequently.
8	How frequently do Ministries meet to discuss future planning on cyber security?	Never	Occasionally – When required	Periodically – Annually	Regularly – Twice annually	Very regularly – Quarterly or more
9	How effectively does your Ministry engage cooperatively with international partners on cyber security? (E.g. ASEAN, Australia, etc.)	Not effective / Unknown – The Ministry does not engage with international partners to cooperate on cyber security.	Limited effectiveness – The Ministry engages with international partners when required, often informally.	Moderately effective – The Ministry engages in regular, informal cooperation programs with international partners on cyber security.	Effective – The Ministry engages in frequent, formal cooperation programs and discussions with international partners on cyber security.	Very effective – The Ministry engages in consistent and formal discussions with international partners on cyber security with a single point of contact. The outcomes of these initiatives are assessed.
10	How frequently does your Ministry engage with international partners on cyber security information	Never / Unknown – The Ministry does not engage with international partners	Occasionally – Informal information sharing when required.	Often – Frequent informal information sharing on high-level information.	Regularly – Frequent formal information sharing on cyber	Very regularly – Frequent information sharing within multilateral agreements on cyber

	sharing? (E.g. ASEAN, Australia etc.)	on cyber security information sharing.			security at the tactical level.	security posture, tactics, and cybercrime.
Cyber Security Governance						
Question		Answer Options				
11	What level of cyber security measures are in place at your Ministry or organization? Cyber security measures may include multi-factor authentication, backups of important data, and application control	Limited - My Ministry or organization applies limited cyber security measures and those that are applied are done when required, or are outdated.	Average - My Ministry or organization has some cyber security measures in place but are applied inconsistently or are considered after a risk/threat has been identified.	Good - My Ministry or organization has cyber security measures in place. However, the maturity of these cyber security measures is still developing.	Very Good - My Ministry or organization has mature cyber security measures in place that are aligned with international standards/frameworks such as ISO.	Excellent - Mature cyber security measures aligned with international standards/frameworks are in place. These are up to date and dynamically adapt to changes in the cyber security environment.
12	How often does your Ministry or organization review its cyber security measures?	Never/Unknown - My Ministry or organization does not conduct reviews of its cyber security posture.	Occasionally - Reviews occur infrequently.	Often - Reviews occur frequently but there is no formal review process in place.	Regularly - Formal review process in place that is conducted frequently.	Very regularly - The review process is formal and adapts to changes in the cyber security environment.
13	What understanding do you have of your Ministry or organization's cyber security policy?	No understanding - I do not understand the requirements of the cyber security policy or there is no cyber security policy.	Limited understanding - I understand some of the requirements of the cyber security policy	Good understanding - I have an overview level understanding of all the requirements of the cyber security policy.	Very good understanding - I understand all requirements of the cyber security policy.	Excellent understanding - I understand all requirements of my cyber security policy and contribute to the strengthening of the cyber security requirements.

14	The roles and responsibilities described in the Cambodian Government's approach to cyber security are:	Not defined or I do not know them.	Somewhat defined - Roles and responsibilities for cyber security are decided on when required.	Mostly defined - The roles and responsibilities for cyber security are broadly defined.	Well defined - Roles and responsibilities for cyber security are defined in an understandable and clearly divided format.	Clearly defined with expectations - Roles and responsibilities for cyber security are clearly defined in an understandable way with clearly defined expectations.
Capacity-Building Awareness						
Question		Answer Option				
15	Cyber security courses and training programs offered by the Government are available to which of these groups? (select all that apply)	Your Ministry or organization's ICT staff	All of your Ministry or organization's staff	Everyone in the Government	Private industry	Citizens/the public
		None of these	I don't know	Other (please specify)		
16	Please describe your cyber security awareness.	I have limited awareness of cyber security and do not know anything about malicious threats and/or mitigations to defend against them.	I have some awareness of cyber security. I sometimes understand malicious threats and/or mitigations to defend against them.	I have a good awareness of cyber security. I mostly understand threats and/or mostly know potential mitigations to defend against them.	I have very good awareness of cyber security, which I keep up-to-date. I understand threats and can provide risk assessments for them and how they may impact the organisation. I am comfortable developing effective mitigations to defend against threats.	I have excellent awareness of cyber security, which I keep up-to-date. I comprehensively understand threats and can provide detailed risk assessments and research looking at how they may impact the organization. I am able to identify potential mitigations to defend against threats and have enough cyber

						security skills to implement mitigations myself or lead a team to do so. I am able to remain flexible and adapt solutions when necessary.
17	Cyber security-specific training and education programs in Government are: Cyber security awareness training may include phishing and password education, authorized use of systems, relevant scams. Cyber skill training may include digital forensics, threat monitoring, and incident response.	Limited - The Ministry has provided no cyber security-specific training to my colleagues.	Average - The Ministry occasionally conducts cyber security awareness training.	Good - The Ministry regularly conducts cyber security awareness training and specific cyber skills training.	Very good - The Ministry frequently conducts cyber security awareness training and cyber skills training. Training is aligned with internationally recognized certifications/accreditations.	Excellent - The Ministry conducts frequent cyber security awareness training and specific cyber skills training. Different types of training are offered to staff with different responsibility levels. Training is updated regularly to ensure relevance with current and emerging technological developments and the threat landscape.
18	Cyber security awareness campaigns run by Cambodian Government agencies for the general public are:	Limited - Cyber security awareness campaigns are not conducted for the public.	Average - Conducted on an improvised basis through limited communication channels	Good - Available through online resources and easily identifiable for users who want information on cyber security.	Very Good - The Government has mechanisms in place to identify the most relevant communication channel depending on target audience to	Excellent - The Government consults with behavioural experts to tailor cyber security awareness campaigns towards the target audience.

					maximise outreach and engagement.	
19	Does your Ministry or organization engage in cyber security research and development projects? How frequently?	Never / Unknown - My Ministry or organization does not engage in cyber security research and development projects.	Occasionally - My Ministry or organization engages in cyber security research and development projects when required.	Often - My Ministry or organization engages in cyber security research and development projects frequently	Regularly - My Ministry or organization's cyber security research and development projects are planned, frequent, and include other ministries.	Very Regularly - My Ministry or organization's cyber security research and development projects are planned, frequent, and include national and international partners.
20	How does your Ministry or organization determine what areas are the priority for research and development? Research and development priorities are key cyber security capabilities or knowledge that are identified by the Government as priorities that need to be developed.	Never / Unknown - My Ministry or organization does not engage in cyber security research and development projects	My Ministry or organization performs improvised studies of cyber security capability conducted when required to identify research and development priorities.	My Ministry or organization follows a defined, consistent, and methodical process that aligns with previously derived priorities.	My Ministry or organization follows a defined, consistent, and methodical process that aligns with all relevant strategic and economic objectives.	My Ministry or organization follows a defined, consistent, and methodical process that aligns with all relevant strategic and economic objectives. It is informed by international trends and developments.
Legal and Regulatory Cyber Security						
Question		Answer Options				

21	Does your Ministry or organization have a methodology for identifying and protecting critical information infrastructure? Please rate how well it is defined.	Limited - Critical information infrastructure is not identified or protected.	Average - Critical information infrastructure is identified and protected when required.	Good - Critical information infrastructure is identified and protected according to a broad methodology.	Very Good - Critical information infrastructure is identified and protected according to a clear methodology that is well defined.	Excellent - Critical information infrastructure is identified by a clear methodology that adapts to new and emerging infrastructure.
22	What is your Ministry or organization's capacity to support cyber security risk management for critical information infrastructure? Please rate the capacity. Critical information infrastructure includes data, database, network, communications infrastructure	Limited - My Ministry or organization does not provide any cyber security guidance for critical information infrastructure providers.	Average - My Ministry or organization provides broad guidance on its online platforms for critical information infrastructure providers.	Good - My Ministry or organization provides support for critical information infrastructure providers to strengthen their cyber security.	Very good - My Ministry or organization provides cyber security guidelines and requirements for critical information infrastructure providers.	Excellent - My Ministry or organization has established cyber security guidelines and requirements for critical information infrastructure providers. These are frequently updated according to the cyber security environment.
23	Does your Ministry or organization have a methodology for identifying and protecting digital service providers? Please rate how well it is defined. Digital service providers are entities that provide digital services built on a networked ecosystem of consumers. (e.g. online search engines, online marketplaces, cloud computing services, etc.)	Limited - Digital service providers are not identified or protected.	Average - Digital service providers are identified and protected when required.	Good - Digital service providers are identified and protected according to a broad methodology	Very Good - Digital service providers are identified and protected according to a clear methodology that is well defined.	Excellent - Digital service providers are identified and protected according to a clear methodology that is defined in detail. The methodology is updated regularly and adapts to new and emerging digital services.

24	How accessible is a reporting platform for Cambodian Government Ministries or private organizations to report a cyber security incident? A very accessible reporting platform provides an easy to navigate website, online portal or software where users can report incidents in real-time.	Inaccessible - Reporting platform does not exist, users report cyber incidents to the applicable individual at the time.	Somewhat accessible - Reporting platform available to only senior Government staff.	Moderately accessible - Reporting platform available to all Government staff.	Accessible - Reporting platform available to all Government staff and private organizations.	Very accessible - Reporting platform is in real-time and available to all Government staff, private organizations, and the public.
25	How effectively is information on cyber security incidents shared between ministries and private organizations?	Not effective - Information is not shared between ministries and private organizations.	Limited effectiveness - Information sharing channels are developing and information is often not received or not clear.	Moderately effective - Information is shared between ministries and private organizations sometimes. Information is mostly clear.	Effective - Information is shared between ministries and private organizations effectively and on a regular basis. Information is always clear.	Very effective - Information is shared between ministries and private organizations, effectively and very regularly. Information is shared in real-time in a clear, uniform format.

Cyber Security Incident Response

Question		Answer Options				
26	When did you most recently assist with a cyber security incident? A cyber security incident is a possible breach of security policy or a security situation that has a significant risk of damaging business operations.	Never have	Over a year ago	In the past year	In the past 6 months	In the past month

27	If you have assisted with a cyber security incident, please provide some details on the incident.					
28	When did you last read, exercise, or review your cyber security incident response plan?	We do not have a cyber security incident response plan.	Over a year ago	In the past year	In the past 6 months	In the past month
29	If a cyber security incident occurred, at what point would you escalate managing the incident to another person?	Immediately upon discovering signs of an incident.	After determining severity or after initial triage.	At a specific phase after or during containment.	After or during containment after discovering a problem I was not confident in solving.	I would not escalate at any point.
30	If you have assisted with a cyber security incident in the past, please describe the actions you performed.					
31	Please describe the process you would follow to escalate the incident.					
32	Please explain your understanding of the difference between triage and containment during cyber security incident response.					

Appendix B Relevant Engagements In The Region

Previous CCTCP projects and their learnings provide valuable insight for developing and implementing more successful capability development projects. CyberCX will adopt learnings from previous engagements to provide more effective education and training methods and resources for Phase 2.

CCTCP and CyberCX – National Bank of Vanuatu

The Challenge: Cyber security resilience and uplift within the National Bank of Vanuatu through technical assessments and training.

What Happened: Engaged by DFAT, CyberCX provided penetration testing services, advice, and support to the National Bank of Vanuatu to achieve Payment Card Industry compliance (PCI DSS) and security uplift of their systems for ISO 27001 certification. Staff skills and awareness was enhanced using Phriendly Phishing and Keep Safe 5 cyber security training products.

Outcomes: The CyberCX team and the National Bank of Vanuatu staff worked together to establish a culture of security for the bank going forward.

CCTCP and Australian National University (ANU) – Cyber Bootcamp Project (CBP)

The Challenge: Addressing cyber challenges and building cyber capacity across a breadth of cyber affairs, at national and regional levels in Indo-Pacific regions

What Happened: Engaged by DFAT within Australia's CCTCP, ANU's National Security College delivered Cyber Bootcamps to several Indo-Pacific regions, with more bootcamps still to be run.

The CBP strengthens understanding of cyber terminology, internet architecture, security policies and strategies for coordinating national cyber policy. It increases awareness of cyber threats, region-specific challenges and promotes the application of the international stability framework for cyber security.

Three bootcamps were intended to be run each year for four years, which includes a two-week intensive program held in Australia. Due to the COVID-19 pandemic, these have been transitioned to virtual settings.

Outcomes: ANU teams have facilitated several virtual, Cyber Bootcamps, with the most recent being with Cambodia in late 2021.

Appendix C Bibliography

Article19 2014, 'Cybercrime Law', Kingdom of Cambodia. https://www.article19.org/wp-content/uploads/2018/02/Draft-Law-On-CyberCrime_Englishv1.pdf

The Association of Southeast Nations 2020, 'ASEAN Digital Masterplan 2025', The Association of Southeast Asian Nations.

Australia's International Cyber and Critical Tech Engagement Strategy, April 21, 2021, Commonwealth of Australia, Department of Foreign Affairs and Trade.

Cheung, B November 2009, 'Criminal Code: Khmer-English Translation', Kingdom of Cambodia. 183-186.

Cimpanu, C November 8, 2018, 'Cambodia's ISPs hit by some of the biggest DDoS attacks in the country's history', ZDNET, <https://www.zdnet.com/article/cambodias-isps-hit-by-some-of-the-biggest-ddos-attacks-in-the-countrys-history/>

Cambodia country brief n.d., Department of Foreign Affairs. <https://www.dfat.gov.au/geo/cambodia/cambodia-country-brief>

Development assistance in Cambodia n.d., Department of Foreign Affairs. <https://www.dfat.gov.au/geo/cambodia/development-assistance/development-assistance-in-cambodia>

Heng, M & Hwang, G October 2019, 'Analysis of Strategic Priorities for Strengthening Cyber Security Capability of Cambodia', *Journal of Digital Convergence*, vol. 17, no. 10: 93-102.

India-Cambodia Bilateral Relations February 5, 2020, Indian Ministry of External Affairs. https://www.mea.gov.in/Portal/ForeignRelation/India-Cambodia_Bilateral_Brief_feb_2020.pdf

'Law on Telecommunications', November 2015, Kingdom of Cambodia.

'Leveraging Investments in Broadband for National Development: The Case of Cambodia' 2018, UN-OHRLS. <https://www.un.org/ohrlls/sites/www.un.org.ohrlls/files/cambodia-broadband-case-study-unohrlls-2018.pdf>

Minges, M, Gray, V & Firth, L March 2002, 'Khmer Internet: Cambodia Case Study', International Telecommunication Union Geneva Switzerland. https://www.itu.int/ITU-D/ict/cs/cambodia/material/KHM_CS.pdf

Nguon, S, & Sopheak, S January 2020, 'Cambodia v. Hackers: Balancing Security and Liberty in Cybercrime Law', Konrad Adenauer Stiftung.

'Outcomes of the 14th ASEAN-Japan Cybersecurity Policy Meeting' October 22, 2021, Ministry of Economy, Trade and Industry. https://www.meti.go.jp/english/press/2021/1022_001.html

Rinith, T December 17, 2020, 'MPTC warns of hackers' attack on Cambodian Telegram users', *Khmer Times*, <https://www.khmertimeskh.com/50794217/mptc-warns-of-hackers-attack-on-telegram-users/>

Sarri, A, Kyranoudi, P, Thirriot, A, Charelli, F, & Dominique, Y December 2020, 'National Capabilities Assessment Framework', European Union Agency for Cybersecurity. DOI: 10.2824/590072.

Schwab, K October 2019, 'Global Competitiveness Report 2019', World Economic Forum. https://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf

The Science, Technology and Innovation Ecosystem of Cambodia August 2021, United Nations Economic and Social Commission for Asia and the Pacific.

Spokesman of TRC October 2021, 'Mobile Internet Subscribers 2021 (Oct)', Telecommunication Regulator of Cambodia, <https://www.trc.gov.kh/en/internet-subscribers/>

'Summary on Cambodian ICT Masterplan 2020' 2014, Korea International Cooperation Agency (KOICA).

END OF DOCUMENT

