STRATEGY

TO INCREASE THE PUBLIC OFFICERS' OVERALL READINESS ON INFORMATION AND CYBERSECURITY

2021

Prepared By

Multi Tech Solutions (Pvt) Ltd.

Table of Contents

Introduction

The strategical foundation for the improvement of national cyber security awareness of the public sector employees was formulated after a thorough survey and analysis conducted. The prior report prepared on Assessment of Public Officials' Information and Cyber Security Readiness Across the Country with respective to its concluding results and analysis was taken to identify the gap analysis with respective to the expected level of awareness together with context analysis.

As all the countries are facing cyber threats in different scales within each territory and all governments provide due attention on the cyber security and information security awareness among their systems under purview. Sri Lanka as a country need to formulate and strengthen information and cybersecurity awareness among its public sector employees when look towards acceleration of digitization of government sector services and operations. Current situation has led all the Nations to provide critical attention on Cybersecurity and invest on preventive measures of Cybersecurity including Sri Lanka. There is a say that "prevention is better than cure", hence, evaluation and prepare the readiness of any nation towards global challenges with respective to the Cybersecurity is a responsibility of all the governments.

When focusing towards the National strategy on uplifting public officers' awareness, there is a need of front-end analysis by considering the desirable state of Cybersecurity awareness among the government officials. Further, the education, official status and duties done by the officers are also diversified into various categories. Therefore, the theoretical framework of the study has been formulated by considering the international programs on Cybersecurity including British Computer Society programs and Cybersecurity Modules developed on Doha Declarations by the UNODC (UNODC-E4J, 2019) (BCS, 2019). In the input category of the employees are categories based on both the National Qualifications and Occupational level. Hence, tools were designed to capture necessary variables with respective to Cybersecurity awareness in line with universally accepted knowledge clusters.

Background

There is no international definition on cybercrime or cyber-attacks. Cybercrime is generally taken into the following forms:

i) offences against the confidentiality, integrity and availability of computer data and systems;
ii) computer-related offences;
iii) content-related offences;
iv) offences related to infringements of copyright and related rights.

In general, cybercrime can be described as cyber-related crime, authorized cybercrime, and, as a certain type of crime, exploitation including child sexual abuse on the Internet (UNODC, 2019).

- Cyber-assisted Cybercrime requires an ICT infrastructure and is often characterized by the creation, dissemination and use of malware, ransomware. Attacks on critical National infrastructures (such as Cybercrime seizures of a power plant by an organized criminal organization) and Cybercrime Offline website by overloading it with data (a DDOS attack) also fall under the same category.
- Cyber-enabled Cybercrime is what can happen in the offline world but can also be facilitated by ICT. This usually includes online scams, online drug purchases and online money laundering.
- Child Sexual Exploitation and Abuse includes abuse on the clear internet, darknet forums and, increasingly, the exploitation of self-created imagery via extortion - known as "sextortion".

According to the (Grayson Kemper, 2019), 34% of people experienced a breach of their personal data in 2017, yet less than half checked to see if their personal data was compromised or whether someone adjusted their privacy settings on social media during that period. This data doesn’t mean people don’t care about privacy or security; they want information to be protected. The problem, instead, is with Cybersecurity awareness, understanding and compliance. The personal struggle that people experience with Cybersecurity directly connects to Cybersecurity in the workplace employees pose the greatest Cybersecurity threats to organizations (Nurse, 2019).

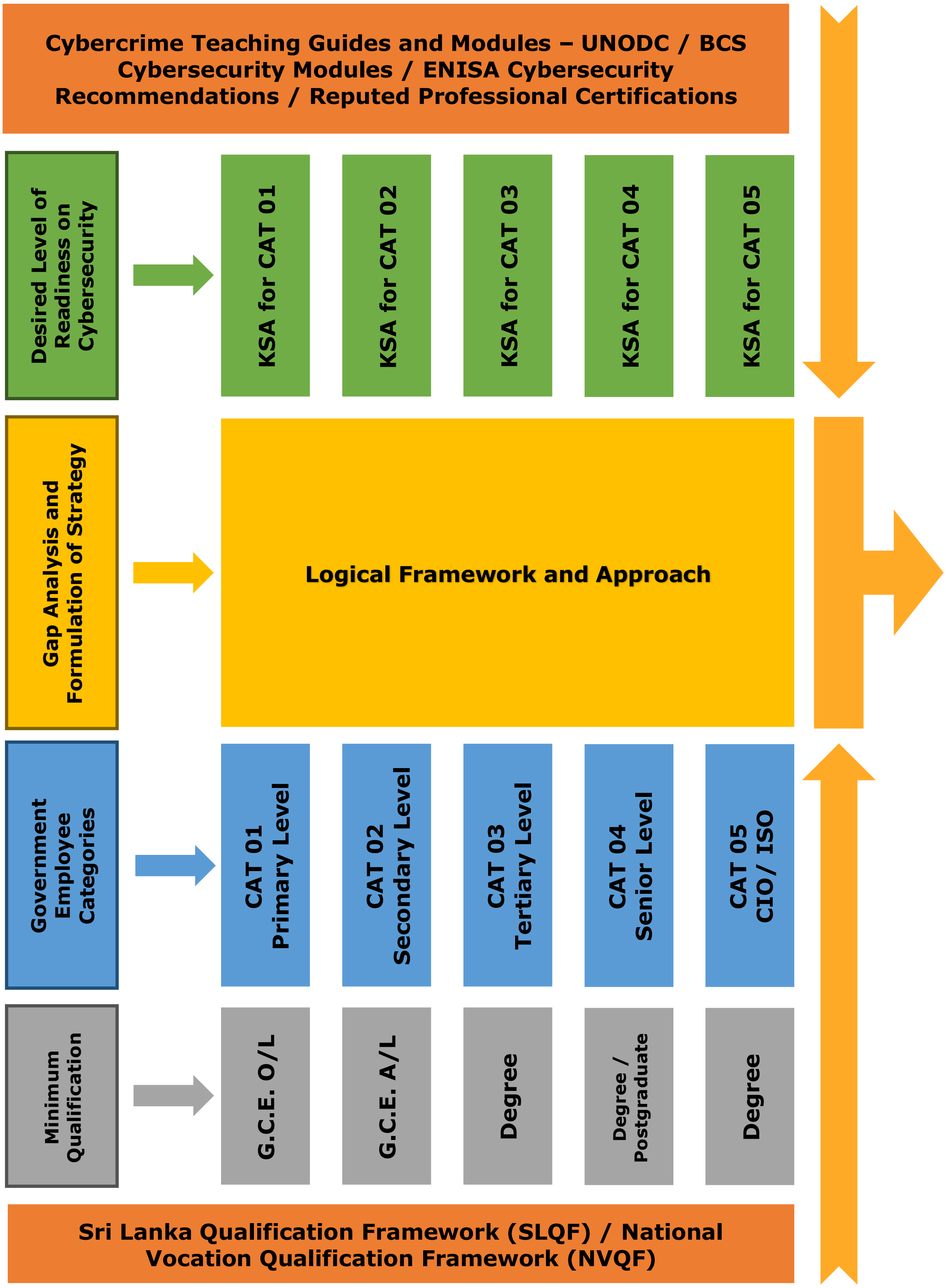
This issue is worsened by the changing cyber threat landscape: the faces of cybercrimes are advancing with new technologies such as artificial intelligence (AI), data science, human behaviors and are constantly presented with new attack faces, due to the growth and grip of the Internet of things (IoT). To limit employee threats, organizations need to emphasize employee awareness of Cybersecurity. There is a trend in targeting Cybersecurity attacks on high- profile and/or revenue-earning organizations. This can be seen by analyzing the recent attacks (Nurse, 2019). To achieve successful awareness of Cybersecurity risk, management of organizations must stress the critical nature of Cybersecurity and implement policies to enforce their positions, rather than dismiss its validity as a threat (Grayson Kemper, 2019).

On 27 June 2019, the European Cybersecurity Act entered into force, setting the new mandate of ENISA (European Network and Information Security Agency), the EU Agency for Cybersecurity, and establishing the European cybersecurity certification framework

(ENISA, 2019). In this legal enactment, while providing security enforcement directions, it also empowers its European cybersecurity certification framework for the governance and rules for EU-wide certification of ICT products, processes and services. Certification plays a critical role in increasing trust and security in products and services that are crucial for the Digital Single Market. At the moment, a number of different security certification schemes for ICT products exist in the EU. But, without a common framework for EU-wide valid cybersecurity certificates, there is an increasing risk of fragmentation and barriers in the European Single Market. Under the purview of ENISA, there are two key tasks. The first being knowledge and information: to provide analyses and advice and to raise awareness, to become the one-stop shop (InfoHub) for cybersecurity information from the EU Institutions and bodies; next is on Capacity building: to reinforce support to EU Member States in order to improve capabilities and expertise, for instance on the prevention of and response to incidents (ENISA, 2019).

These activities and the operation within different context and prominent bodies emphasize the relationship among awareness of Knowledge, Skills, Attitudes (KSA) in tandem with vulnerabilities, victimizations and threats of Cybercrimes prevalent in society. Therefore, the enhancement of awareness becomes critical for any Nation vying for Cybersecurity readiness status. Providing strategy to uplift necessary awareness levels, demands analysis of the current situation beforehand. By considering all of the above cases, following theoretical framework has been formulated as the first phase of study. It is also meant to identify gaps in awareness and understand continuous improvement deemed necessary for Cybersecurity readiness purposes.

Conceptual Framework


Cybercrime Teaching Guides and Modules – UNODC / BCS Cybersecurity Modules / ENISA Cybersecurity Recommendations / Reputed Professional Certifications
Desired Level of Readiness on Cybersecurity
KSA for CAT 01
KSA for CAT 02
KSA for CAT 03
KSA for CAT 04
KSA for CAT 05
Gap Analysis and Formulation of Strategy
Logical Framework and Approach
Government Employee Categories
CAT 01 Primary Level
CAT 02 Secondary Level
CAT 03 Tertiary Level
CAT 04 Senior Level
CAT 05 CIO/ ISO
Minimum Qualification
G.C.E. O/L
G.C.E. A/L
Degree
Degree / Postgraduate
Degree
Sri Lanka Qualification Framework (SLQF) / National Vocation Qualification Framework (NVQF)

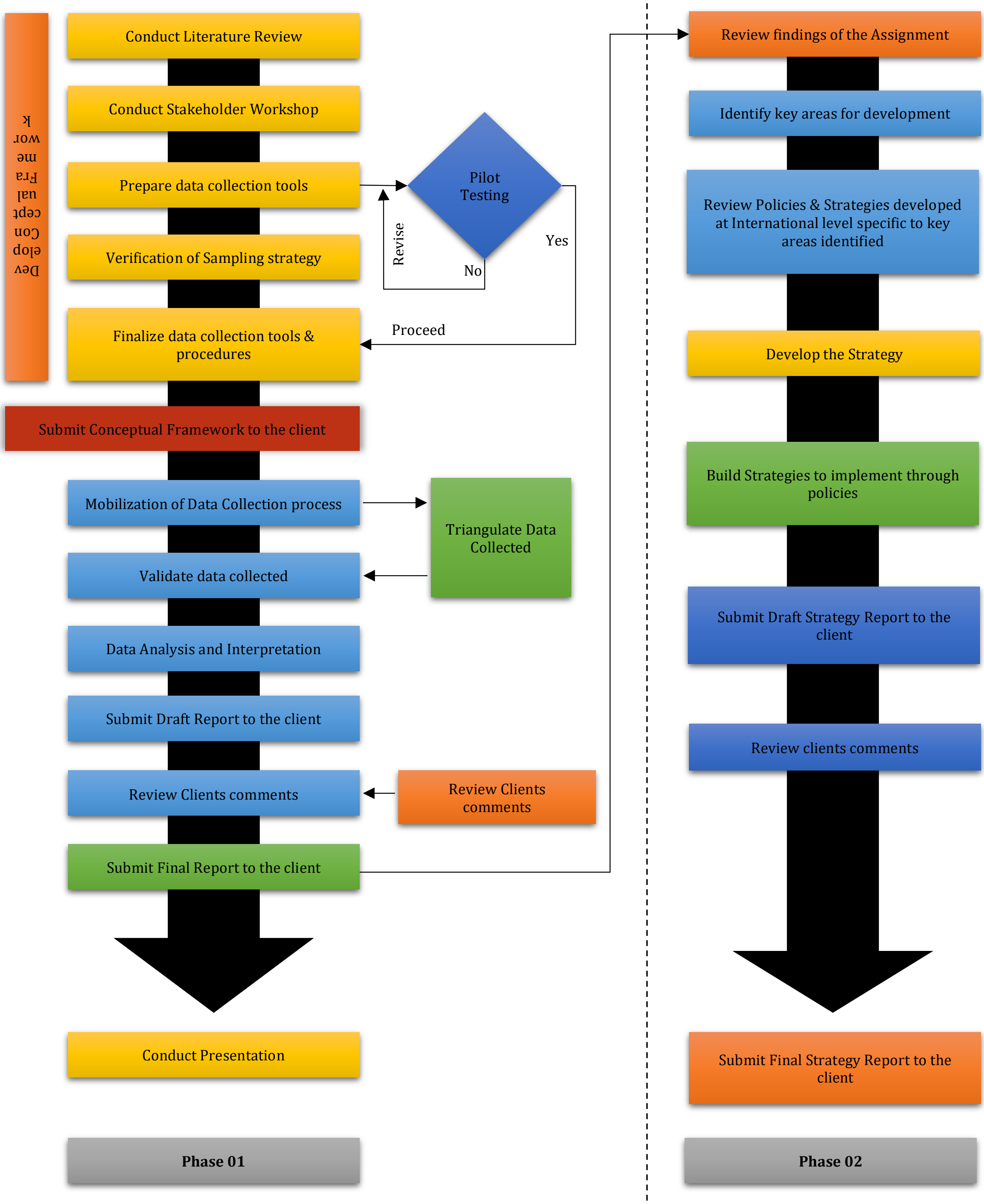
Initially, the government employee categories were classified into 5 distinct categories based on Government Public Administrative and Management Circular number 3/2016, issued by Secretary to the Ministry of Public Administration and Management (Secretary, 2016) (Treasury, 2006). These circulars indicate four main employee categories which are common across the entire government employee system. A special category defined by SLCERT and ICTA Sri Lanka which is known as CIO/ISO separately coming under the Tertiary level (CERT, Draft Cyber Security Act 2019, Sri Lanka, 2019) (ICTA, 2019). Has also been taken into consideration in categorizing Government Employees.

Further, the minimum required qualifications of employees have also been considered under each category with respect to circulars (Secretary, 2016) and (Treasury, 2006). In order to maintain a National level cohesive framework, the identified minimum qualifications have been mapped with the Sri Lanka Qualification Framework (SLQF) and the National Vocational Qualification Framework (NVQF) (Lanka, 2015) (Commission, 2015).

For analysis purposes, both qualitative and quantitative techniques are to be used encompassing five categories of public employees proportionately. The data gathering techniques are elaborated in the Logical Framework and Approach. Identifying desired levels of awareness on Knowledge, Skills and Attitudes of government officials, has been done in keeping with International standards and guidelines as indicated in the theoretical framework. This again will be considered separately for each and every employee category.

The quantitative and qualitative data will be collected mainly based on the above five employee categories. Based on the analyzed results of both data collected and information collected through consultant team will be used to identify Cybersecurity readiness levels of government officials. The results would then indicate the current awareness levels of government officials. The literature review conducted by experts will also be used to further understand the expected awareness level of knowledge, skill and attitudes needed. Based on the findings, asper the techniques mentioned above, experts will then identify the gap between the current level of Cybersecurity readiness level of government officials and the expected level of Cybersecurity readiness level of government officials. Once the gap is identified by the consultant team, a proposal will be prepared in support of uplifting the Cybersecurity awareness level to the benchmarked level.

Logical Framework and Approach


Develop Conceptual Framework
Conduct Literature Review
Conduct Stakeholder Workshop
Prepare data collection tools
Pilot Testing
Revise
No
Yes
Verification of Sampling strategy
Finalize data collection tools & procedures
Proceed
Submit Conceptual Framework to the client
Mobilization of Data Collection process
Triangulate Data Collected
Validate data collected
Data Analysis and Interpretation
Submit Draft Report to the client
Review Clients comments
Review Clients comments
Submit Final Report to the client
Conduct Presentation
Phase 01
Review findings of the Assignment
Identify key areas for development
Review Policies & Strategies developed at International level specific to key areas identified
Develop the Strategy
Build Strategies to implement through policies
Submit Draft Strategy Report to the client
Review clients comments
Submit Final Strategy Report to the client
Phase 02

Design Rationale for the Data Gathering Tools

According to the glossary of United States National Initiative for Cybersecurity Careers and Studies, Cybersecurity is extensively defined as "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation". The definition is further elaborated as "Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure" (Studies, 2018). These definitions highlight vital aspects that need to be considered in the context of cybersecurity.

Public officers survey is a foundation metric used to evaluate the awareness of employees, staff and other members of government institutions. To evaluate the current readiness, it is vital to elicit awareness on necessary key elements and their coverage of Cybersecurity in accordance with respective officers' perspectives.

Considering information security as a key term, there are three widely accepted elements referred to as the "CIA Triad". The key elements are Confidentiality, Integrity and Availability (Recoverability) of information. It also addresses both Physical Security and virtual Security. Security awareness surveys have been conducted by many organizations as well as many professional organizations such as ITU, SANS, ISACA, and ISC. Vulnerability of the "human element" is still considered as the weakest link in security (Kamal Dahbur, 2017).

Under the common CIA pillars, in general, officers according to their respective roles and responsibilities must be knowledgeable on the following:

- ***People***: Public officers must be educated and trained to enhance their knowledge, skills, and attitude with regard to security.
- ***Technology***: Technology in both software and hardware must be up-to-date, in addition it should be secure and user-friendly. Public officers must be trained on technology based on their respective job roles and responsibilities. Technology should also be selected and configured properly to facilitate the implementation of functionality without compromising security.
- ***Processes and Procedures***: Processes must be designed and implemented to regulate the use of technology by public officers based on their respective job roles and responsibilities. Procedures must be defined and implemented as per the guidelines of best-practices to promote effectiveness of processes.
- ***Policies***: Policies must be clearly defined, using high-level statements that all public officers can understand, to achieve the security objectives of the institution. Management must also be committed to the enforcement of the policies to ensure organizational compliance and their effectiveness.

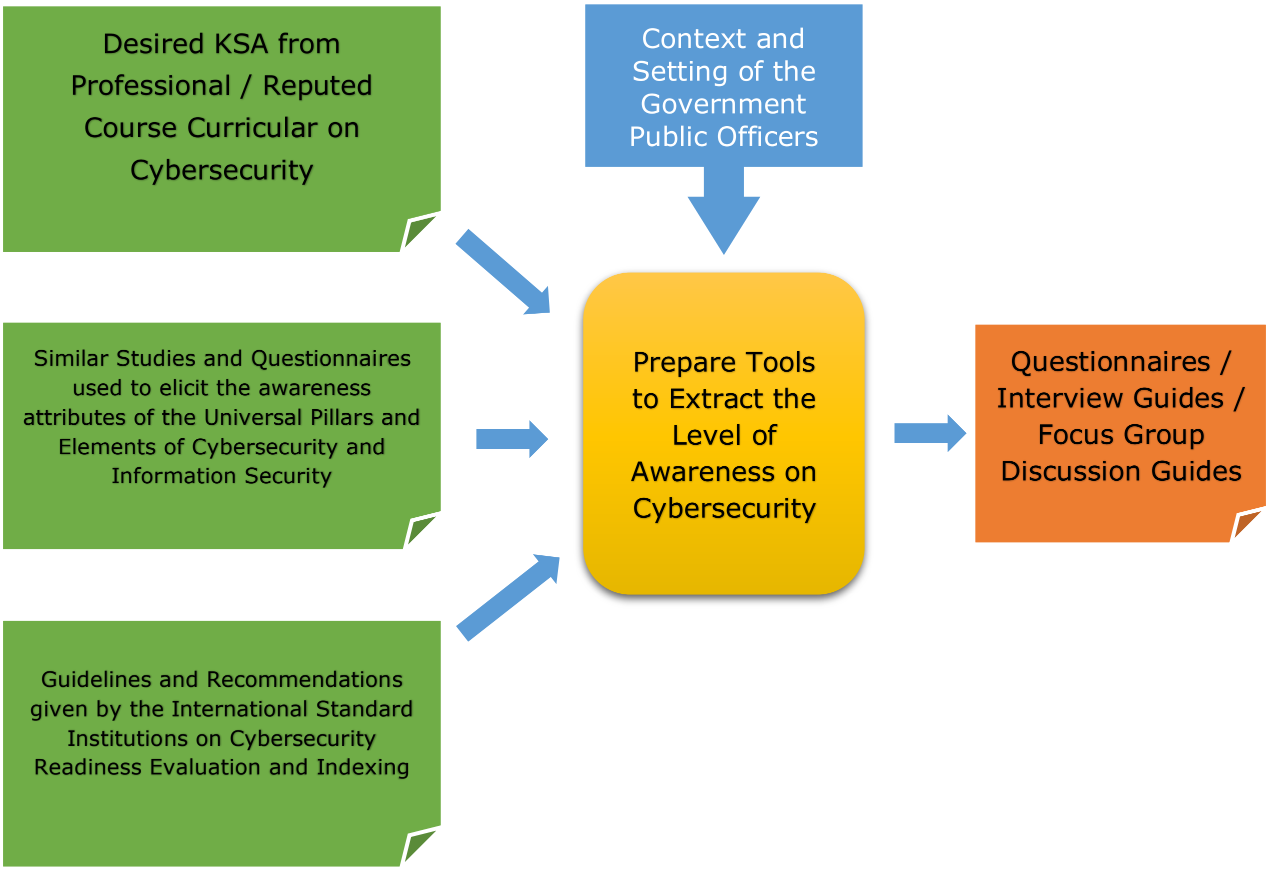
Above four elements are in par with the five indices used by ITU/BDT Cybersecurity Programme for Global Cybersecurity Index (GCI) Reference Model and their Global Cybersecurity Index 2018 Questionnaire Guide (ITU/BDT Cyber Security Programme,

2018) (Union, 2018). It is vital to consider the relationship of government officers' awareness related to 5 aspects, namely Legal Measures, Technical Measures, Organizational Measures, Capacity Building, and Cooperation which are used for Global Cybersecurity Indexing purposes; however, all 25 sub-indices are not directly related to individual public officers' awareness levels in executing their respective job roles.

Further to the necessary Cybersecurity elements, in deriving the awareness level under each component, the desired attributes were examined and extracted by investigating several standard professional courses and guides provided by reputed institutes such as BCS, ITU and UNODC (BCS, 2019) (UNODC-E4J, 2019) (Union, 2018).

The conceptual model of deriving the questionnaires for the four public officer groups, interview discussion questions identification, and focus group session guides were derived through the flow of the following conceptual model.

Conceptual Model for the Preparation of Data Gathering Tools


Desired KSA from Professional / Reputed Course Curricular on Cybersecurity

Context and Setting of the Government Public Officers

Similar Studies and Questionnaires used to elicit the awareness attributes of the Universal Pillars and Elements of Cybersecurity and Information Security

Prepare Tools to Extract the Level of Awareness on Cybersecurity

Questionnaires / Interview Guides / Focus Group Discussion Guides

Guidelines and Recommendations given by the International Standard Institutions on Cybersecurity Readiness Evaluation and Indexing

Sampling Frame

It is composed of three stages and final stage derive the number of officials to be surveyed. Multi Stage Stratified Random Sampling technique will be used in this assignment to cover all the sectors of public organizations including all categories of public officials as the assignment is based on evaluating Cybersecurity readiness of all the public officials in the country.

Stage 1

In this stage category of employer will be considered as the stratification factor and therefore, all public sector officials will be categorized into four strata's as listed below;

- National Ministries and Institutions grouped under Ministries
- Provincial Councils and Institutions grouped under Provincial Councils
- District Secretariats and Institutions grouped under District Secretariats
- Institutions not grouped under a Ministry

Each stratum will be designed with a specific theoretical framework and the final strategic plan will also be developed for each of those stratums separately.

Strata	Definition
Line ministries and Institutions grouped under line Ministries	Employees who are currently employed in government and Semi Government agencies coming under the Line Ministries are provided by the name of the Ministry
Provincial Councils and Institutions grouped under Provincial Councils	Information is provided separately for all 9 Provincial Councils. Under each Provincial Council, separate information is given for the Chief Secretariat which includes all independent institutions in that particular Provincial Councils as well as 5 Provincial Ministries
District Secretariats and Institutions grouped under District Secretariats	Employees who are currently employment in District Secretariats and other institutes grouped under District Secretariats are given under the respective District Secretariat. Each District Secretariat comprises the staff in the District Secretariat premises, Divisional Secretariats as well as the Vidatha Centres/Divineguma Praja Moola Banks/ Cultural Centres in Divisional Secretary's Divisions
Institutions not grouped under a Ministry	Aggregated information on Government agencies and Semi Government agencies that belong to the Central Government but not coming under a Line Ministry is provided. This consists of the Presidential Secretariat, Prime Minister's Office, Parliament and independent officers located in the Parliament Complex, The Supreme Court, Court of Appeal, Election Commission, Judicial Service Commission and its Courts, Audit Service Commission, National Police Commission, Human Rights Commission, Finance Commission, National Procurement Commission, Delimitation Commission etc. and other independent institutions

As per the report generated by Department of Census and Statistics on Census of Public and Semi Government Sector Employment – 2016 following data was extracted for each of the Strums identified above.

#	Stratum	No of Employees by Sex - 2016		
		Male	Female	Total
1	National Ministries and Institutions grouped under Ministries	416,036	200,128	616,164 (58.80%)
2	Provincial Councils and Institutions grouped under Provincial Councils	145,968	239,090	385,058 (34.87%)
3	District Secretariats and Institutions grouped under District Secretariats	37,056	52,908	89,964 (8.15%)
4	Institutions not grouped under a Ministry	6,768	6,265	13,033 (1.18%)
Total		**605,828**	**498,391**	**1,104,219**

**Census of Public and Semi Government Sector Employment – 2016 (Department of Census and Statistics)*

Stage 2

Total Sample Size:

A total number of 7000 public officials will be consider as the total sample size of this study to estimate the public officials' information and Cybersecurity readiness in Sri Lanka.

The government institute will be considered as a primary sampling unit and 15 randomly selected employees of each selected institutes will be the secondary sampling units. Further, it is important to find the gap and formulate the strategy for Readiness on Cybersecurity for each category of employees. Therefore, selection of 15 employees in each institute will be further distributed as follows,

Minimum Qualification	Government Employee Categories	Sampling units will be covered per institute
G.C.E. O/L	Primary Level	2
G.C.E. A/L	Secondary Level	8
Degree	Tertiary Level	2
Degree / Postgraduate	Senior Level	2
Degree	CIO/ ISO	1
Total		**15**

**Categories were defined based on the Government Public Administrative and Management Circular number 3/2016, issued by the Secretary to the Ministry of Public Administration and Management* (Secretary, 2016) (Treasury, 2006). *These circulars have indicated the four main employee categories which can be seen in government employee system. Further, it has taken in to the consideration of special category defined by the CERT and the ICTA Sri Lanka which called as CIO/ISO separately which comes under the Tertiary level* (CERT, Draft Cyber Security Act 2019, Sri Lanka, 2019) (ICTA, 2019). *Therefore, the Government Employee categorization was carried out on above basis.*

Service Level	Ministries & Institutes	Provincial Councils & Institutes	District Secretariat & Institutes	Not under any Ministry	Total
Primary	516	322	76	20	**934**
Secondary	2064	1288	304	80	**3736**
Tertiary	516	322	76	20	**934**
Senior	516	322	76	20	**934**
CIO/ ISO	258	161	38	10	**467**
Total	**3870**	**2415**	**570**	**150**	**7005**

Stage 3

In this stage each District will be considered as the second stratification factor in order to identify Demographic (Gender) and Geographic spread/ coverage.

Total number of 10 institutes will be randomly selected out of 20 institutes under stratum Institutions not grouped under a Ministry. Also, Total number of institutes to be covered under each stratum will be calculated by using probability proportional to size (PPS) method.

#	Stratum	No of Employees	Proposed Sample Size	
			No. of Institute	No. of Employees
1	Line ministries and Institutions grouped under line Ministries	616,164 (58.80%)	258	3870
2	Provincial Councils and Institutions grouped under Provincial Councils	385,058 (34.87%)	161	2415
3	District Secretariats and Institutions grouped under District Secretariats	89,964 (8.15%)	38	570
4	Institutions not grouped under a Ministry	13,033 (1.18%)	10	150
Total		**1,104,219**	**467**	**7005**

Revised Sample

At the time of proposal development attention was given for accuracy & precision and less consideration was given for cost, time and staff constrains. The behavior /variation of main variables of the study were also not perfectly known at the initial stages of the study. Based on the available information and the stakeholder requirements it was decided to go for a large sample size of 7005 respondents.

According to the situation prevailed due to COVID 19 pandemic it was not possible to carryout field operation as planned. With the great efforts made by all the stakeholders of this project it was possible to complete 3264 sample units of pre decided sampling frame of 7005 sample units.

It was an urgent requirement to study /test whether the available sample size is sufficient to achieve the final objective of the study. The primary analysis it was revealed that 90 percent of government officers did not know or not using Cybersecurity applications in and around their official environments. Whereas main variable of the study is the assessing awareness of Cybersecurity application of the government officials. Under this situation the following sample size calculation formula was applied to the separate strata to get the total required sample size.

$$\boldsymbol{n} = \frac{\boldsymbol{N z_{\alpha}^{2} P Q}}{\boldsymbol{N E^{2}} + \boldsymbol{Z_{\alpha}^{2} P Q}}$$

Strata	Notations of the equations	Strata 1 line Ministries	Strata 2 Provincial Councils	Strata 3 District Secretariats	Strata 4 Institutions not grouped under a Ministry
Population Size	N	616164	385058	89964	13033
Expected Knowledge Proportion on Cyber Security	P	0.1	0.1	0.1	0.1
Unknown Knowledge Proportion on Cyber Security	Q =(1-P)	0.9	0.9	0.9	0.9
Expected maximum error	E	0.02	0.02	0.02	0.02
Error Squire		0.0004	0.0004	0.0004	0.0004
.05 Sig. level of St. Normal Distribution	Z	1.96	1.96	1.96	1.96
	Z^2	3.8416	3.8416	3.8416	3.8416
N*Z^2*P*Q		213035.006	133131.4932	31104.51322	4506.0816
N*E^2		246.4656	154.0232	35.9856	5.2132
Z^2*P*Q		0.345744	0.345744	0.345744	0.345744
N*E^2+Z^2*P*Q		246.811344	154.368944	36.331344	5.558944
Sample Number	n	863	862	856	811
Total Sample Size		**3392**			

Aa a result of above calculations the total scientific sample size should be the 3392 units whereas the total number completed was 3264. According to the results the sampling error is only 128. (i.e., 3392-3264 = 128)

At the same time, it is to understand that the available stratified sample sizes are large enough to central limit theorem (i.e., $n > 30$) of the statistics and it is possible to undertake any statistical hypothesis testing if required. Therefore, it is derived that that the new sample size is scientifically valid to arrive at statistically accepted conclusions.

Highlights on Awareness level of Government Employees on Information and Cyber security

When considering the outline findings reported in the Assessment of Public Officials' Information and Cyber Security Readiness Across the Country with respect to the survey result analysis of the current status of government employees respective to the information and cyber security awareness, it can highlight that;

- Majority (73%) has obtained some-type of ICT based education. However, ICT education has not influenced on their Cybersecurity KSA.

- However, Primary category of employees have shown very low-level exposure to the formal ICT education or training.

- Very poor ICT security related policy level awareness was observed: Generally, Fair usage (88%), Information security (82%), social media (83%), User access (83%), Data security (83%), and Disaster recovery (89%) policies are not available in the majority of the organizations.

- ICT education or Cyber security related education/training has not influenced on all the practices that was tested in this survey.

- Very fewer (6%) has Cybersecurity education or training were obtained by the sample. However, Cybersecurity training/education has not influenced on their KSA level.

- While having this type of policy level freedom and lower KSA levels in cybersecurity, Government employees are not using information technology in a subsequent manner. Consequently, there is a grave danger of going towards E-Government or digitalization.

- Primary and Secondary category employees are enrolling in using ICT in their offices (E.g., documentation). This population do not have a proper KSA level on Cybersecurity applications, specifically primary category employees. This imposes a higher risk on Cybersecurity.

- General awareness of Cybersecurity threats also shown in very low level where it stresses a properly planned upliftment of KSA regarding cybersecurity through formal trainings.

Further when considering the ICT officers who are currently assigned in their respective office places, the following findings were observed.

- Majority of employees who are handling ICT related work in organizations are system administrators (30.9%) and other officers (53.9%). According to findings, it seems they do not have required level of technical knowledge or skills to handle Cybersecurity related work.

- Small No. of CIOs are available, and out of them majority comprised a standard level of knowledge and skills compared to other ICT officers on Cybersecurity.

- In an average of less than 40% had a basic security knowledge, which shows about less than 20% had knowledge on system protection.
- Approximately, 20-25% had awareness on ICT asset identification, asset classification, and asset inventory classification, and less than about 20% had taken actions to secure their organizational assets.

- Employees who had an awareness on ICT asset identification, classification, and inventory, less than 40% were implementing the security procedures.

- Approximately, 25-30% of employees comprised awareness on data classification and sensitive data classification. Ministry level ICT related employees have shown the highest awareness compared to other organizations.

- General awareness on ICT policies are very low among employees, and less than about half of employees were involved on making policies and procedures out of which were implemented.

- Approximately, 50% of employees had awareness on operational awareness.

- ICT officers had very low knowledge on Disaster recovery policies, implementation, and current usage.

- Employees had lower awareness on network and application security.

While considering the above gaps in the awareness levels, the following approach is to be modeled to uplift the awareness in general. With respective to the expected level of awareness, the approach was formed with long term strategies supported with sort term foundation strategies to hold the long-term plans.

STRATEGY FORMATION

National expectations to be in line with the global standards of Cybersecurity awareness

According to the Cybersecurity Capacity Maturity Model for Nations (CMM), it helps nations to understand what works, what does not work and why, across all areas of cybersecurity capacity. This is important for any government which can adopt policies and make themselves ready to have the potential to significantly enhance safety and security in cyberspace, while also respecting human rights, such as privacy and freedom of expression.

Based on Global Cyber Security Capacity Center (GCSCC) on their CMM 2021, it refers to five dimensions to be used to evaluate the Cyber Security Readiness. Which all together constitute the breadth of national government workforce capacity that a country requires to be effective in delivering cybersecurity. Those five dimensions are;

1) Developing cybersecurity policy and strategy;
2) Encouraging responsible cybersecurity culture within society;
3) Building cybersecurity knowledge and capabilities;
4) Creating effective legal and regulatory frameworks;
5) Controlling risks through standards and technologies.

When considering the government employees' information and cybersecurity awareness, the expected level of awareness can be obtained based on the maturity model represented in the CMM 2021. When considering the five dimensions of their awareness, those dimensions can be described as,

1) **Developing Cybersecurity Policy and Strategy:**
This explores the country's capacity to develop and deliver cybersecurity strategy, and to enhance its cybersecurity resilience by improving its incident response, cyber defense and critical infrastructure (CI) protection capacities. This Dimension considers effective strategy and policy in delivering national cybersecurity capability, while maintaining the benefits of a cyberspace vital for government, international business and society in general.

2) **Encouraging responsible cybersecurity culture within society:**
Cybersecurity Culture and Society reviews important elements of a responsible cybersecurity culture such as the understanding of cyber-related risks in society, the level of trust in Internet services, e-government and e-commerce services, and users' understanding of personal information protection online. Moreover, this Dimension explores the existence of reporting mechanisms functioning as channels for users to report cybercrime. In addition, this Dimension reviews the role of media and social media in shaping cybersecurity values, attitudes and behaviour.

3) **Building Cybersecurity Knowledge and Capabilities:**
This aspect reviews the availability, quality and uptake of programmes for various groups of stakeholders, including the government employees as a whole, and relate to cybersecurity awareness-raising programmes, formal cybersecurity educational programmes, and professional training programmes.

4) **Creating effective legal and regulatory frameworks:**
Legal and Regulatory Frameworks examines the government's capacity to design and enact national legislation that directly and indirectly relates to cybersecurity, with a particular emphasis placed on the topics of regulatory requirements for cybersecurity, cybercrime-related legislation and related legislation. The capacity to enforce such laws is examined through law enforcement, prosecution, regulatory bodies and court capacities. Moreover, this Dimension observes issues such as formal and informal co-operation frameworks to combat cybercrime.

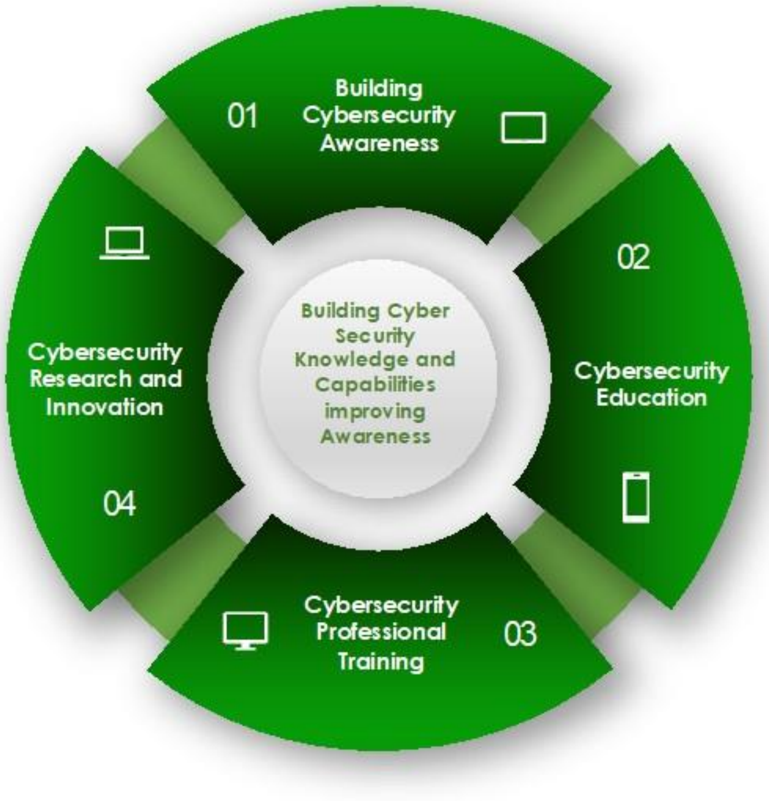
5) **Controlling risks through standards and technologies:**
This examines the Standards and Technologies addresses effective and widespread use of cybersecurity technology to protect individuals, organizations and national infrastructure. This Dimension specifically examines the implementation of cybersecurity standards and good practices, the deployment of processes and controls, and the development of technologies and products in order to reduce cybersecurity risks.

The CMM normally defines five Stages of maturity for all Dimensions being which are taken under start-up, formative, established, strategic, and dynamic. These correspond to the following states which are initial development of capacity, being established, being world-leading, and able to anticipate and prepare for future cybersecurity needs.

It is also noteworthy that there are relationships between these Dimensions. In this aspect of government employee's awareness on information and cyber security is directly referred to the dimension (3) of "Building cybersecurity knowledge and capabilities", however, if other dimensions are lagging behind in their respective status, then awareness building, knowledge creation and capacity building cannot be effective. Hence, it can be clearly seen that to build the awareness of information and cybersecurity for the government sector employees, rely on several aspects. Further, when considering the maturity level, all the levels are depending on good foundation of awareness on cybersecurity. Hence, it is noteworthy that Sri Lanka's government sector current maturity level cannot expected beyond start-up whereas the awareness level of the employees does not show good evidences of maturity.

Approach

When forming the awareness building strategy for the government sector, out of key dimensions discussed above, the third dimension was taken as the core and other dimensions were taken as supporting dimensions where inter dependents. Therefore, all the key strategies were formulated around the third dimension.


01
Building Cybersecurity Awareness
02
Cybersecurity Education
03
Cybersecurity Professional Training
04
Cybersecurity Research and Innovation
Building Cyber Security Knowledge and Capabilities improving Awareness

1) Building Cybersecurity Awareness

This Factor focuses on the availability of programmes that raise cybersecurity awareness throughout the country, concentrating on cybersecurity risks and threats and ways to address them.

Aspects

- ✓ *Awareness-raising Initiatives by Government:* this Aspect targets the existence of a national co-ordinated cybersecurity awareness-raising programme driven by the government, covering a wide range of demographics and issues, developed in consultation with stakeholders from various sectors and experts.
- ✓ *Awareness-raising Initiatives by Private Sector:* this Aspect should target to promote awareness-raising programmes driven by the private sector and the extent to which they are aligned with government and civil society initiatives.

- ✓ *Awareness-raising Initiatives by Civil Society:* this Aspect should be accomplished by facilitating of awareness-raising programmes driven by the civil society and the extent to which they are aligned with government and private sector initiatives.

- ✓ *Executive Awareness Raising:* this Aspect targets to raise executives' awareness of cybersecurity issues in the public, private, academic and civil society sectors, as well as how cybersecurity risks might be addressed.

2) Cybersecurity Education

This Factor addresses the availability and provision of high-quality cybersecurity education programmes and sufficient qualified teachers, trainers and lecturers. Moreover, this Factor examines the need to enhance cybersecurity education at national and institutional levels and the collaboration between government and industry to ensure that educational investments meet the needs of the cybersecurity education environment across all sectors.

Aspects

- ✓ *Provision:* this Aspect can cover through educational cybersecurity offerings and educator qualification programmes available that provide an understanding of current risks and skills requirements.

- ✓ *Administration:* this Aspect can cover through co-ordination of, and resources for developing and enhancing cybersecurity education frameworks with allocated budget and spending based on the national demand.

3) Cybersecurity Professional Training

This Factor can facilitate by making the availability and provision of affordable cybersecurity professional training programmes to build a cadre of cybersecurity professionals. Moreover, this Factor can uptake cybersecurity training, and horizontal and vertical cybersecurity knowledge and skills transfer within organizations, and how this transfer of skills translates into a continuous increase of cadres of cybersecurity professionals within the government sector.

Aspects

- ✓ *Provision:* this Aspect can cover through development, availability and provision of cybersecurity training programmes for enhancing skills and capabilities.

- ✓ *Uptake:* this Aspect show the uptake and affordability of such programmes to produce a cadre of certified cybersecurity professionals. Issues investigated include initiatives to register for such programmes, initiatives to retained the employees after successful completion, knowledge sharing after completing a programme, and the existence of a national register of successful and certified students.

4) Cybersecurity Research and Innovation

This Factor addresses the emphasis placed on cybersecurity research and innovation to address technological, societal and business challenges and to advance the building of cybersecurity knowledge and capabilities in the country specifically in the government sector.

Aspects

- ✓ *Cybersecurity Research and Development:* this Aspect can promote the existence of a research and innovation culture in the country's government employee's knowledge penetration and innovative ways of skill cyber readiness through one that is related to a national list of current and completed projects, financial support, incentives and usable research outputs.

In line with the above mechanisms to uplift governmental maturity on Cybersecurity, awareness building must be done through key educational and training programs with a correct approach of stirring the motivation of the employees of the government sector.

Trainings and awareness are to be prepared in accordance with the aim of strengthening and building the foundation on key awareness of the following areas where the survey results have revealed the weak level of representation of awareness of each aspect. It is true that as a country, some of the following areas are not established yet where awareness cannot be expected without such establishment.

1) Cybersecurity Policy and Strategy

- ➥ National Cybersecurity Strategy
- ➥ Incident Response and Crisis Management
- ➥ Critical Infrastructure (CI) Protection
- ➥ Cybersecurity in Defense and National Security

2) Cybersecurity Culture and Society

- ➥ Cybersecurity Mindset
- ➥ Trust and Confidence in Online Services
- ➥ User Understanding of Personal Information Protection Online
- ➥ Reporting Mechanism
- ➥ Media and Online Platform

3) Building Cyber Security Knowledge and Capabilities

- ➥ Building Cybersecurity Awareness
- ➥ Cybersecurity Education
- ➥ Cybersecurity Professionals Security
- ➥ Cybersecurity Research and Innovation

4) Legal and Regulatory Frameworks

- ➥ Legal and Regulatory Provisions
- ➥ Related Legislative Frameworks
- ➥ Legal and Regulatory Capability and Capacity
- ➥ Formal and Informal Co-Operation Frameworks to Combat Cybercrime

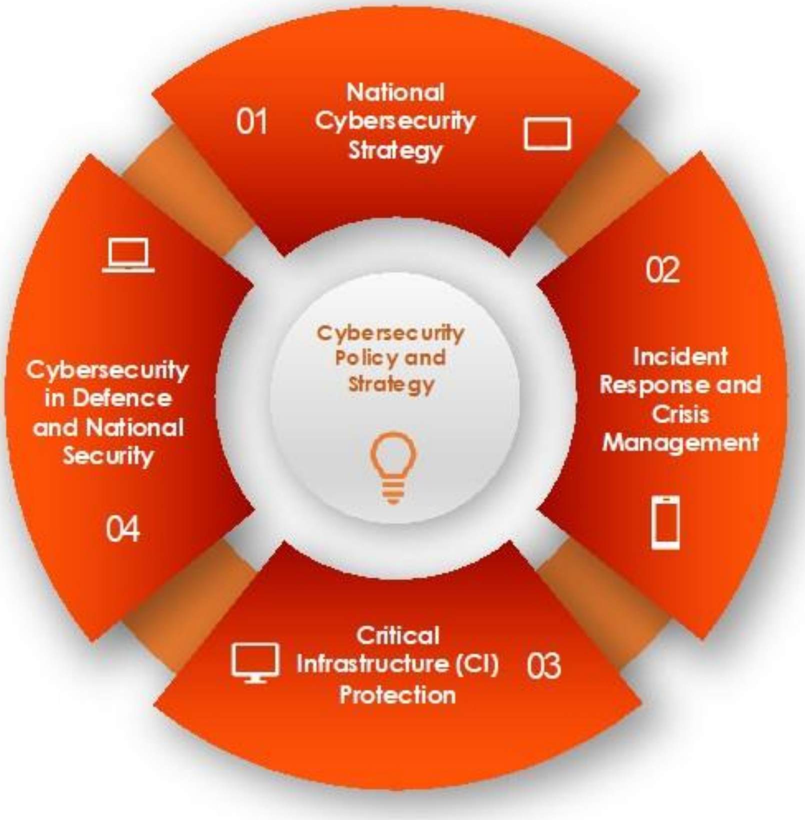
5) Standards and Technologies

- Adherence to Standards
- Security Controls
- Software Quality
- Communications and Internet Infrastructure Resilience
- Cybersecurity Marketplace
- Responsible Disclosure

Other Associated Demotions

Dimension 1:

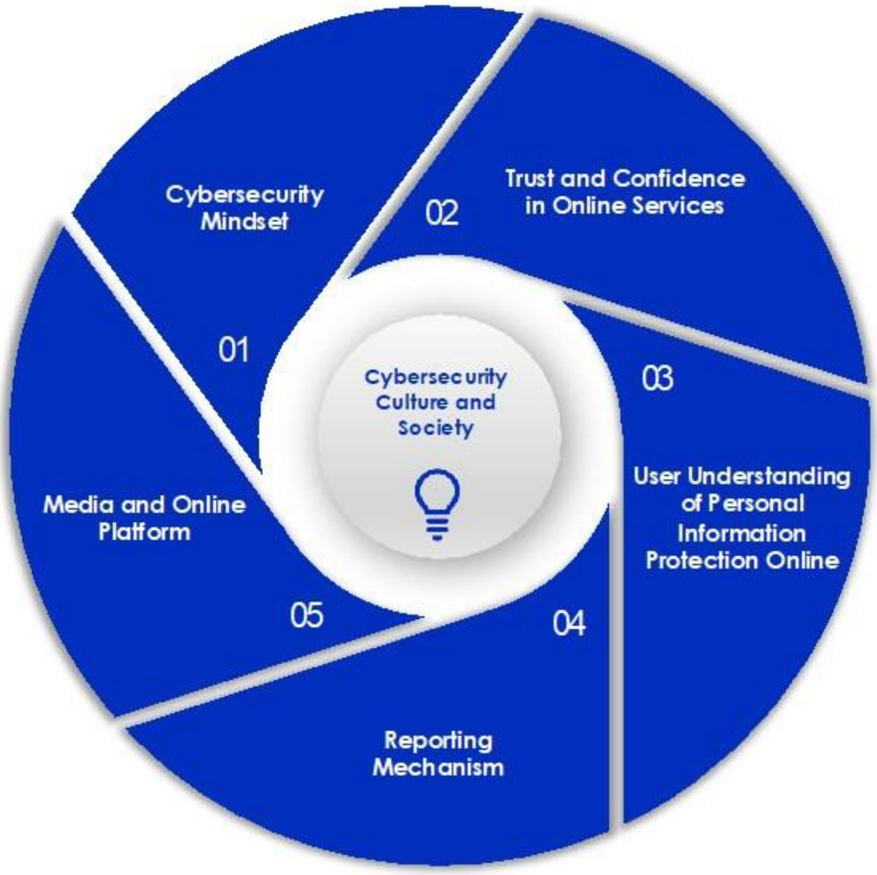
There is a critical need of introducing colossal level policy framework for the government sector with respective to ICT, information, and cybersecurity policy. Then the policies which are applied to various organizations based on criticality and the context, those are to be made aware to the employees through a peer group or institutionalized internal programs. A employee participatory mechanisms would be highly beneficial when forming the policies through national level policy framework where natural awareness could be built.


Cybersecurity Policy and Strategy
01
National Cybersecurity Strategy
02
Incident Response and Crisis Management
03
Critical Infrastructure (CI) Protection
04
Cybersecurity in Defence and National Security

At activity level of policy implementation, main focusing functions could be introduced as:

- Competency (Through peer sharing)
- Penetration testing (User feedback mechanisms and active UAT setups)
- Frequent awareness (Institutionalized knowledge sharing and peer coaching)
- Monitoring and evaluation
- Incident reporting mechanism (Preparation of standard procedures with forms/tools)
- Alerting system
- Password policy and protection

Dimension 2:


Cybersecurity Mindset
01
Trust and Confidence in Online Services
02
03
User Understanding of Personal Information Protection Online
04
Reporting Mechanism
05
Media and Online Platform
Cybersecurity Culture and Society

A cybersecurity culture is lead through the awareness of the benefits of standard practices and operations. The security culture could be established through proper awareness on the benefits, advantages, and various encouragement mechanisms.

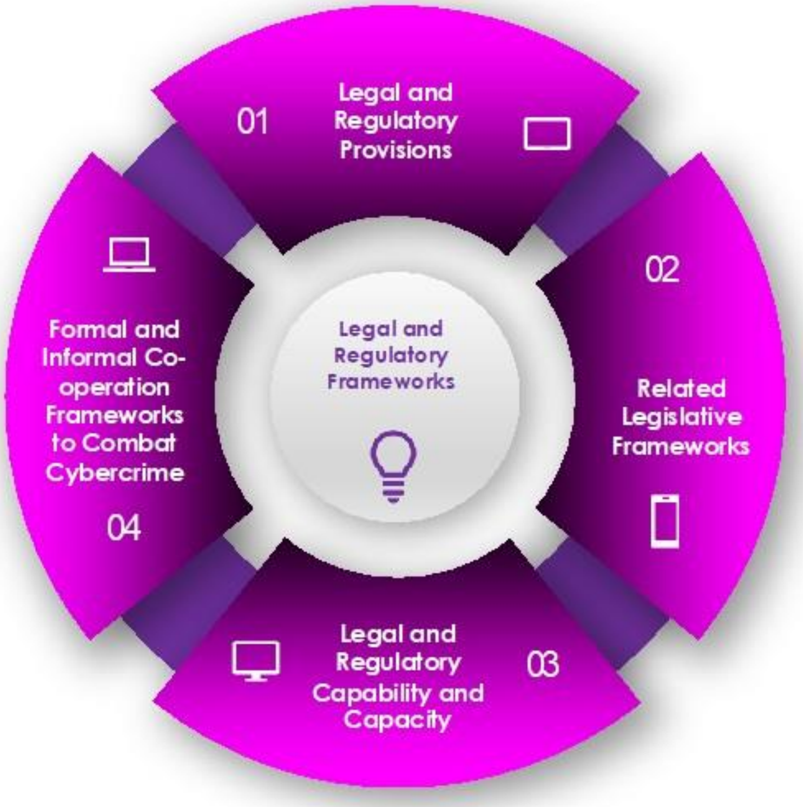
Implementation activities could be focused on:

- Cybersecurity knowledge raising workshops
- Introduction of online modules for distance learning
- Awareness campaign over social media

Dimension 4:

Without a proper legal and regularity framework, expectation of awareness is a myth. Therefore, first a legal and regulatory framework are to be established through expert consultations where individual organizations should adopt with their own context in an appropriate manner with respective to their applicability. A participatory decision-making mechanism can enhance understandability of the requirement of such frameworks and also governing principles among the employees.

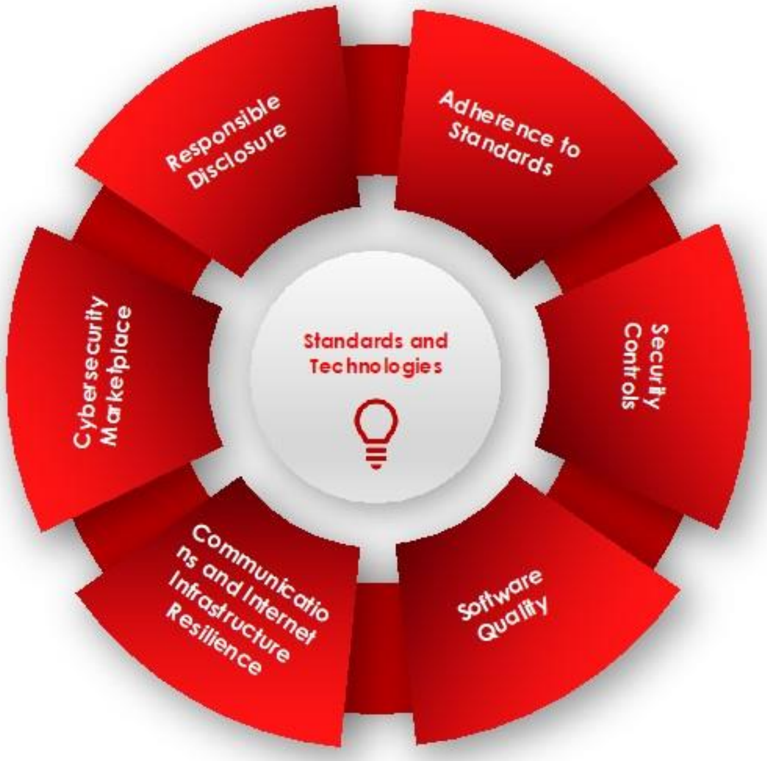
Establishing the appropriate legal infrastructure is an integral component of a national cybersecurity strategy.



Legal and Regulatory Frameworks
01
Legal and Regulatory Provisions
02
Related Legislative Frameworks
03
Legal and Regulatory Capability and Capacity
04
Formal and Informal Co-operation Frameworks to Combat Cybercrime

Dimension 5

Development of cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures, as well as addressing the approach to organizing national cybersecurity efforts.


Standards and Technologies
Responsible Disclosure
Adherence to Standards
Security Controls
Software Quality
Communications and Internet Infrastructure Resilience
Cybersecurity Marketplace

This nature of awareness could be given only for the ICT officers or high-tech professionals who are responsible of technical aspects of the organizations.

Module Objectives as per the expectations of the level of achievements

As per the identified categories of employees in the government sector, the following levels of Information and Cybersecurity awareness can be built with the respective outcomes. Further, the module objectives for each level also accompanied for the planning and development of awareness programs strategically.

Primary Level	Secondary Level
• Foundation Level • Introduction Level	• Foundation Level • Introduction Level • Introduction to Cybercrime and Types of Cybercrimes
Tertiary Level	**Senior Level**
• Foundation Level • Introduction Level • Introduction to Cybercrime • General Types of Cybercrimes • Legal Frameworks and Human Rights • Cybersecurity and Cybercrime Prevention	• Foundation Level • Introduction Level • Introduction to Cybercrime • General Types of Cybercrimes • Legal Frameworks and Human Rights • Cybersecurity and Cybercrime Prevention • Information and Cybersecurity policy formation and Implementation
ICT Officers	
• Cybersecurity and Cybercrime Prevention: Practical • Privacy and Data Protection • Interpersonal Cybercrime • Last Level: (Technologist skill level)	

1. Foundation Level

Objectives

Trainees should be able to demonstrate an understanding of information and cyber security foundations.

➥ **Learning Outcomes:**

- Explaining the importance of cyber security and basic concepts of cyber security including harm, identity, confidentiality, integrity, availability, threat, risk and hazard, trust and assurance and the 'insider threat'.
- Explaining how the concepts relate to each other and the significance of risk to a business.
- Understanding and proposing appropriate responses to current and new attack techniques, hazards and vulnerabilities relevant to the network and business environment.
- Understanding and proposing how to deal with emerging attack techniques, hazards and vulnerabilities relevant to the network and business environment.

2. Introduction Level

Objectives

Apprentices should be able to demonstrate an understanding of the foundations of cyber security.

- **Learning Outcomes:**
  - Describe and explain why information and cyber security are important to business and to society.
  - Describe and explain the terminology and basic concepts of cyber security.
  - Demonstrate and explain the concept of information assurance and how it can be delivered.
  - Describe and explain how security objectives can be developed and used to build a security case.
  - Demonstrate and explain how the basic security concepts can be applied to typical information and communications technology (ICT) cyber infrastructures.
  - Describe and explain common attack techniques and sources of threat.
  - Illustrate and explain ways to defend against the main attack techniques.
  - Describe and explain legal, regulatory, information security and ethical standards relevant to the cyber-community.
  - Discover and explain the concept and practice of keeping up with the threat landscape (horizon scanning).
  - Describe and explain future trends in cyber security.

3. Introduction to Cybercrime and Types of Cybercrime

Information and communication technology (ICT) has transformed the way in which individuals conduct business, purchase goods and services, send and receive money, communicate, share information, interact with people, and form and cultivate relationships with others. This transformation, as well as the world's ever-increasing use of and dependency on ICT, creates vulnerabilities to criminals and other malicious actors targeting ICT and/or using ICT to commit crime. This Module content introduces key concepts relating to cybercrime, what cybercrime is, Internet, technology and cybercrime trends, and the technical, legal, ethical, and operational challenges related to cybercrime, different types of cybercrime, particularly cybercrimes that are considered offences against the confidentiality, integrity and availability of computer data and computer-related offences, and content-related offences and cybercrime prevention.

- **Learning outcomes**
  - Define and describe basic concepts relating to computing
  - Describe and assess global connectivity and technology usage trends
  - Define cybercrime and discuss why cybercrime is scientifically studied
  - Discuss and analyse cybercrime trends
  - Identify and discuss the categories of cybercrime and the cybercrimes included within these categories
  - Differentiate between different forms of cybercrime
  - Describe and explain the ways in which certain cybercrimes are perpetrated

- Identify, examine, and analyse the technical, legal, ethical, and operational challenges relating to the investigation and prevention of cybercrime

4. Legal Frameworks for Cyber Security

National, regional, and international laws can govern behaviour in cyberspace and regulate criminal justice matters relating to cybercrimes. These laws not only set rules and expectations for behaviour, but also the procedures to be followed if the rules are broken, and behaviour expectations are not met. However, core cybercrime offences in national laws are not harmonized between countries, complicating international cooperation in criminal justice matters.

The focus of this Module content is to describe the legal landscape relating to cybercrime, highlight the need for harmonized legislation, and outline the relationship between cybercrime laws and human rights. As this content shows, cybercrime laws need to be following human rights law, and any limitation of a human right needs to be in accordance with human rights standards and principles.

↣ **Learning outcomes**

- Identify, discuss, and examine the need for and role of cybercrime laws
- Describe and differentiate between substantive, procedural, and preventive cybercrime laws
- Identify and critically assess national, regional, and international cybercrime laws
- Critically evaluate the protection of human rights online

5. Cybersecurity and Cybercrime Prevention

Strategies, Policies and Programmes

Information and communication technology (ICT) is integral to national and global development by facilitating innovation and economic growth. The ever-increasing interdependency of digital devices within countries, as well as growing network connections with the digital systems of other countries, has made ICT vulnerable to cybercrime. Because cybercrime can adversely impact national security, international security, and the global economy, the protection of ICT is considered of paramount importance nationally and internationally. In view of that, countries worldwide have published strategies delineating how ICT will be protected from cybercrime and cybercriminals.

↣ **Learning outcomes**

- Discuss Internet governance and identify and assess Internet principles, conflicts that arise in the realization of these principles, and barriers to universal Internet governance
- Describe the basic features of cybersecurity strategies and differentiate between cybersecurity and cybercrime prevention strategies
- Explain and evaluate the objectives and lifecycle of national cybersecurity strategies

- Identify, examine, and evaluate frameworks for international cooperation on cybersecurity matters
- Assess national and international efforts to enhance countries cybersecurity posture

6. Cybersecurity and Cybercrime Prevention: Practical

Applications and Measures

Cybersecurity refers to the strategies, policies, guidelines, procedures, practices, and measures that are designed to identify threats and vulnerabilities, prevent threats from exploiting vulnerabilities, mitigate the harm caused by materialized threats, and safeguard employees, property, and information.

↣ **Learning outcomes**

- Define, discuss, and evaluate assets, threats, vulnerabilities, and risks
- Identify and assess the ways in which vulnerabilities can be disclosed
- Describe and critique the relationship between cybersecurity and usability
- Discuss situational crime prevention and apply it cybercrime prevention and reduction
- Discuss and analyse incident detection, response, and recovery

7. Privacy and Data Protection

Personal data is sought by both criminals and cybercriminals and used in the commission of crime and cybercrime. This personal data can be obtained from a variety of sources. This personal data can reveal information about individuals' age, race, ethnicity, nationality, gender, religious and political beliefs, sexual orientation, thoughts, preferences, hobbies, medical history and concerns, psychological disorders, profession, employment status, military service, affiliations, relationships, geolocation, habits, routines, and other activities, among other information. This personal data, when aggregated, can provide an almost complete picture of individuals' personal and professional lives.

Specifically, this Module content can cover privacy as a human right, the relationship between privacy and security, the ways in which cybercrime compromises privacy and data security, and data protection and breach notification laws, as well as the ways in which data is (and can be) protected to secure persons, property, and information.

↣ **Learning outcomes**

- Discuss privacy and its importance as a human right
- Identify and analyse the impact of cybercrime on privacy
- Critically evaluate the relationship between security and privacy
- Critique data protection and breach notification laws and practices across nations
- Critically assess data protection enforcement practices of states and recommend effective ways to protect data

8. Interpersonal Cybercrime

Information and communications technology (ICT) provides innumerable opportunities for participation in civic and political affairs and social activities and has the potential to individuals with access to education and economic prospects, irrespective of their geographic location. ICT also provides users with immeasurable opportunities to communicate with others and share information. These opportunities, however, can be misused by others to sexually exploit and abuse children and adults, perpetrate anti-social and aggressive acts, and incite violence and other forms of aggression at individuals, groups and/or targeted populations to cause harm to others.

- **Learning outcomes**
  - Define interpersonal cybercrime
  - Define and differentiate between types of interpersonal cybercrime
  - Describe and analyse the ways in which information and communication technology is used to facilitate these types of interpersonal cybercrime
  - Identify and critically engage with the role of law in addressing these cybercrimes
  - Recognize and assess the obstacles to preventing and responding to various interpersonal Cybercrimes

9. Skills for the Cyber Security Technologist

The qualifications are designed for employees enrolled on Cyber Security Technologist level (ICT Officers), to provide them with the technical knowledge and understanding they require for their role detailed below:

The primary role of a Cyber Security Technologist is to apply an understanding of cyber threats, hazards, risks, controls, measures and mitigations to protect organizations systems and people. Those focused on the technical side work on areas such as security design & architecture, security testing, investigations & response. Those focused on the risk analysis side focus on areas such as operations, risk, governance & compliance. Whether focused on the technical or risk analysis side, all people in this occupation work to achieve required security outcomes in a legal and regulatory context in all parts of the economy. They develop and apply practical knowledge of information security to deliver solutions that fulfil an organization's requirements.

Apprentices will develop an understanding and be able to have factual, procedural and theoretical knowledge of fundamental Cyber Security theory, techniques, risk analysis and law.

Apprentices undertaking the 'Technologist' learning pathway will develop skills and be able to demonstrate the following topics: Showing an understanding of basic networks and security components; data protocols; how to build a security case; good design practice; common security architectures; show an appreciation for reputable security architectures (to incorporate hardware and software components); security controls and threats; basic cryptography and key legal issues.

Apprentices undertaking the ‘Risk Analysis’ learning pathway will develop skills and be able to demonstrate an understanding of Cyber Risk assessment methodologies; threats; threat trends; audit and assurance; cryptography and its main techniques; the significance of key management and appreciate the associated legal standards, regulations and ethical standards relevant to cyber security.

Apprentices should be able to demonstrate: logical and creative thinking; analytical and problem-solving skills; an ability to work independently and to take responsibility using their own initiative; show an ability to work with a range of internal and external people; have an ability to communicate effectively in a variety of situations and maintain a productive, professional and secure working environment.

Strategical Implementation Plan

The key stakeholders or drivers to enhancement of awareness level government sector is its employees. The positive participation and motivation are a key factor to the success of the entire effort of cybersecurity awareness enhancement. As per the date, there is a lack of coverage of cybersecurity within the ICT programs which are recognised through various institutions. There is not any encouragement or career prospectus towards achieving such awareness improvement. This can be considered as major threat for the leveraging the awareness on cybersecurity among the government employees. Therefore, it is proposed to introduce motivational factor through an efficiency bar mechanism to achieve required level of KSA through awareness or training programs.

Efficiency bar with basic training

Sometimes, this type of concept is a mostly required one when comparing to the outcome of other training programme. If the targeted group has no commitment or motivation to be trained, then all the efforts will be diminished. Some of ICT knowledge creation is already included in the efficiency bar exams. Therefore, this strategy could encourage participants to learn skills and get knowledge on Cybersecurity. Accordingly, GOSL must establish a recognized certificate programmes which embodied into efficiency bar.

Use of Existing Facilities for Awareness Improvement Plan

As far as awareness building of government sector employees is a national level massive effort related project, the necessary facilities to cater the need are to be considered thoroughly. Mainly the infrastructure facility, ease of access, and skill full human resources are to be considered. As the first marching can be considered through the general education sector-based mechanism where, 10155 schools available island wide and 3519 IT labs are operated by 7471 teachers in all districts. This can be considered as one way to reach the government employees in a long run.

No of Schools	10155
IT Labs	3519
Teachers	7471

However, there are few short comings also can be seen when selecting schools where morning time slots cannot be used and only weekends and evening can be used for the programs. Further, the equipment and facilities may not match with the required level of trainings. The IT teachers may not be able to transform into adult trainers and qualification offering and certification also may be new to school system.

When considering the Technical Vocational Education and Training (TVET) sector institutions, they also have island wide fully equipped infrastructure better than general education system. The following table lists the approximate number of labs available in each district.

District	No. of Labs
Ampara	22
Anuradhapura	13
Badulla	7
Batticaloa	23
Colombo	23
Galle	21
Gampaha	22
Hambantota	17
Jaffna	13
Kalutara	12
Kandy	16
Kegalle	12
Kilinochchi	6
Kurunegala	19
Mannar	4
Matale	7
Matara	12
Monaragala	12
Mullaitivu	3
Nuwara Eliya	11
Polonnaruwa	3
Puttalam	10
Ratnapura	17
Trincomalee	16
Vavuniya	12
Total	**333**

The institutions under TVET are Vocational Training Authority (VTA), National Apprentice and Industrial Training Authority (NAITA), Department of Technical Education and Training (DTET), National Youth Service Council (NYSC) and few other institutions which provide NVQ programs. The IT staff strength also can be seen approximately in the following table.

District	No. of Staff
Ampara	40
Anuradhapura	24
Badulla	13
Batticaloa	34
Colombo	54
Galle	30
Gampaha	66
Hambantota	21
Jaffna	41
Kalutara	16

Kandy	21
Kegalle	17
Kilinochchi	15
Kurunegala	43
Mannar	10
Matale	20
Matara	16
Monaragala	28
Mullaitivu	6
Nuwara Eliya	15
Polonnaruwa	7
Puttalam	9
Ratnapura	32
Trincomalee	32
Vavuniya	19
Total	**629**

These staff members are trained to providing vocational training and matches with certification requirements also. Hence, this NVQ mechanism can be used to introduce the training programs for the Cybersecurity by targeting the above content coverage. However, these staff members are not specially trained for the cybersecurity trainings, hence there should be a short-term strategy to be established through a master trainer program or Training of Trainers program.

The national level acceptance and recognition for the evaluation scheme of the awareness and training programs to be established through the government recruitment and promotion criteria of employees.

Continuous monitoring and evaluation of status score of the cybersecurity awareness among the government sector employees to be done periodically (every year as an quality assurance activity) to measure the impact of the programs.

Short Term Strategical Directives

These short-term strategical directives are help full to form and put the foundation for the long-term action plans and strategies.

- Ready the training resource persons with the target programs and uplift the trainers KSA. Conduct Master Training programs and ToT programs for the selected training institutional trainers.
- Prepare and validate training modules as per the directions given above and obtain NVQ certification levels.
- Convincing the decision makers about cybersecurity readiness requirements and encourage for a national awareness building plan.

- Identify the institutions which are holding critical information and cortical systems and identify key employees to be trained to create multiplier effect within their institutional setup with a short period.
- Complete cybersecurity policy framework for forming policies for government institutions and educate policy makers in the institutions.
- Prior to the development of the framework, following programmes required to be conducted.
    - Executive training program for Policy makers
    - Hire some trained officer to develop policies
- Prepare a media campaign on importance of securing information resources and protecting against attacks. This could be done through social media, TV discussions, newspapers, posters etc.

Master Training Programme

Master trainers could be selected from different ministries, departments, DS offices, and PCs. Once they/targeted group have been selected a training could be provided to the targeted group. The impact of this programme is to enable a multiplayer effect. For instance, if 10 people trained from 10 ministries, each trainer could train 10 more people from his/her ministry, consequently total number of people who acquired training will be 100 at the end of the programme. This kind of programme is easy to design and perhaps it may be the cheapest when considering the budgetary allocations.

It is advisable that TVET IT Trainers can easily be transformed into Master trainers.

The certification can be done through the TVET institutions where it could be achieved through a special governmental project.

Readying for the Future

There is a need of integrating Cybersecurity knowledge into each vocational level program appropriately. This could be done through the support of Technical Vocational Education Commission (TVEC). Further, it is advisable to integrate sufficient level of KSA into ICT degree programs and other inter disciplinary degree programs as appropriate manner to build cybersecurity savvy generation in the future. There is a need of doping some basic aspects of cybersecurity awareness into the school textbooks and make students aware on basics of cybersecurity and forms of crimes.

There should be a mechanism to review and include necessary aspects of cybersecurity awareness certifications into the government scheme of recruitments and promotion schemes.