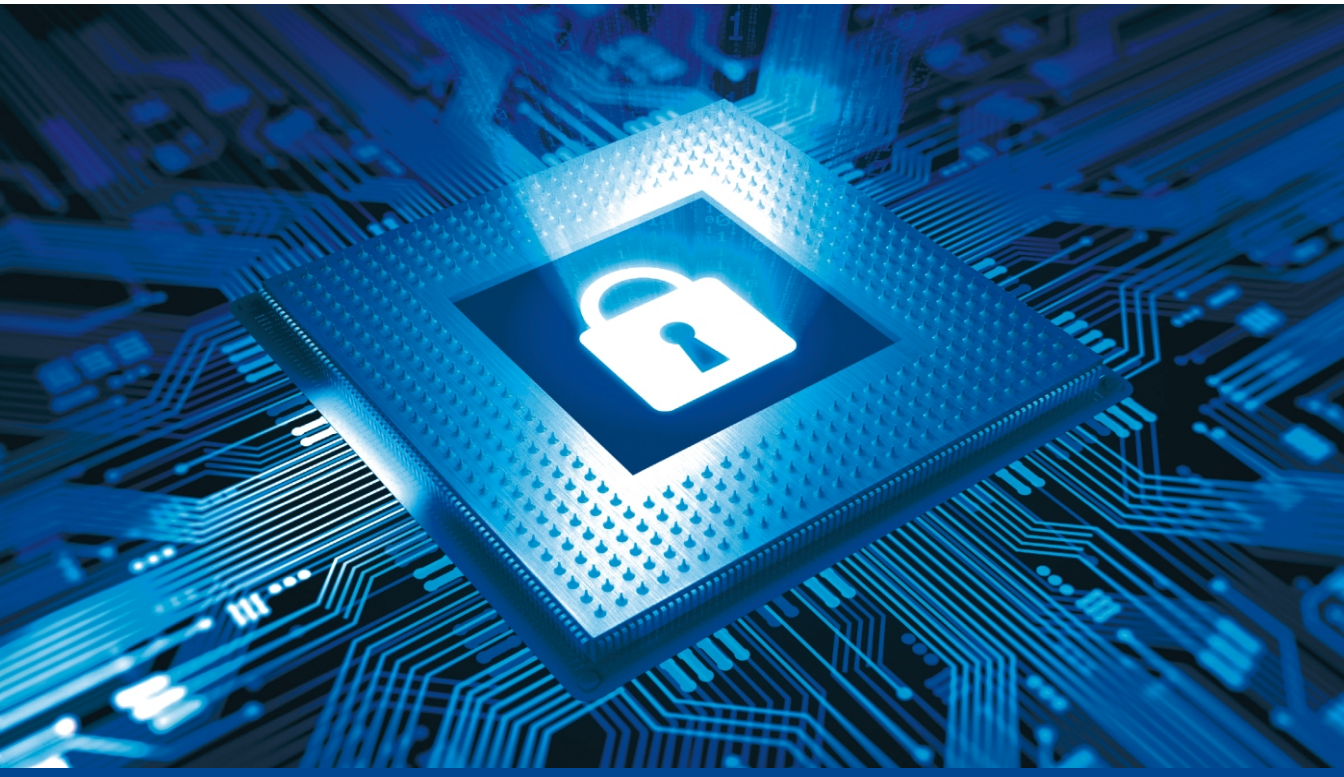
SRI LANKA CERT | CC



Information and Cyber Security Strategy of Sri Lanka

2019 - 2023

National Information and Cyber Security Strategy of Sri Lanka (2019-2023)

November 2018

SRI LANKA CERT | CC

Sri Lanka Computer Emergency Readiness Team | Coordination Centre

Ministry of Digital Infrastructure and Information Technology

Attribution
This publication should be attributed as follows
Democratic Socialist Republic of Sri Lanka, Sri Lanka CERT|CC, *National Information and Cyber Security Strategy of Sri Lanka 2019-2023*, November 2018

Published by
Sri Lanka CERT|CC
First Print: November 2018
Second Print: October 2019

Contact
Enquires about this document are welcome and should be directed to :
Research and Policy Unit
Sri Lanka CERT|CC
Room 4-112, BMICH, Colombo 7,
Sri Lanka.
Telephone: Tel: +94 11 269 1692/269 5749/267 9888
Fax: +94 11 269 1064
Email: cert@cert.gov.lk
Website: www.cert.gov.lk

Design and layout by
Sri Lanka CERT|CC

Table of Contents

Acronyms and Abbreviations

APCERT	Asia Pacific Computer Emergency Response Team
Sri Lanka CERT|CC	Sri Lanka Computer Emergency Readiness Team | Coordination Centre
CII	Critical Information Infrastructure
CIO	Chief Innovation Officer
CIRT	Computer Incident Response Team
CSIRT	Computer Security Incident Response Team
CSP	Certification Service Provider
DIPA	Digital Infrastructure Protection Agency
DoS	Denial of Service
DDoS	Distributed Denial of Service
EGDI	e-Government Development Index
ENISA	European Union Agency for Network and Information Security
FIRST	Forum for Incident Response Security Teams
GCE	General Certificate of Education
GCI	Global Cybersecurity Index
HCI	Human Capital Index
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technology
ICTA	Information and Communication Technology Agency
IP	Internet Protocol
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISOC	Internet Society
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
IWWN	International Watch and Warning Network
M&E	Monitoring and Evaluation
NCA	National Certificate Authority
NCSOC	National Cyber Security Operation Centre
NGO	Non-government Organization
NVQ	National Vocational Qualification
OSI	Online Service Index
TII	Telecommunication Infrastructure Index
TRC	Telecommunication Regulatory Commission
UNIGF	United Nations Internet Governance Forum

Preface

Around the globe, digital technologies have evolved into a powerful economic tool that has improved quality of life of citizens and transformed the way that governments, businesses, and citizens connect, engage, and access information and services. Many societies are now dependent on digital technologies which has led these technologies to be considered as a fundamental social infrastructure.

Along with their numerous benefits digital technologies also bring with them numerous cyber threats. The global number of cyber security incidents recorded in 2015 was 59.06 million[1]. A study estimates that the total annual cost of all data breaches by 2019 will be $2.1 trillion which is almost four times the estimated cost of breaches in 2015[2]. In Sri Lanka, The Sri Lanka Computer Emergency Readiness Team| Coordination Centre (Sri Lanka CERT|CC) received 3907 cyber security related incidents in 2017, which is a significant increase from 2010.

In this context, we, the government of Sri Lanka, seeks to show our commitment to keep the nation safe, secure and prosperous, by introducing Sri Lanka's first Information and Cyber Security Strategy which will be implemented over a period of five years from 2019 to 2023. Our strategy aims to create a resilient and trusted cyber security ecosystem that will enable Sri Lankan citizens to realize the benefits of digital technology, and facilitate growth, prosperity and a better future for all Sri Lankans.

Our strategy is underpinned by six pillars:

1. Establishment of a governance framework to implement the National Information and Cyber Security Strategy
2. Enactment and formulation of legislation, policies, and standards to create a regulatory environment to protect individuals and organizations in the cyber space
3. Development of a skilled and competent workforce to detect, defend and respond to cyber attacks
4. Collaboration with public sector authorities to ensure that the digital government systems implemented and operated by them have the appropriate level of cyber security and resilience
5. Raising awareness and empowering citizens to defend themselves against cybercrimes
6. Development of public-private, local-international partnerships to create a robust cyber-security ecosystem

Analysis of the Present Status

This section presents an overview of the overall ICT readiness, the current status of the digital government initiatives in Sri Lanka, and information and cyber security landscape of Sri Lanka.

Our ICT Readiness

In Sri Lanka IT Literacy is 28.3% and Digital Literacy is 38.7%[3]. Fixed telephone subscription per 100 inhabitants is 12.49, mobile phone subscriptions per 100 inhabitants is 103.16, and broadband subscriptions per 100 inhabitants is 10.45[4]. Household computer ownership is 23.5% while the Internet usage stands at 21.3%, and email usage at 11%[3]. There is a significant disparity in ICT readiness among the Urban, Rural and Estates sectors in Sri Lanka.

Some facts [3,4]

Household Computer Ownership
23.5%
Urban: 39.9%
Rural: 21%
Estate: 5.1%

Telephone Subscriptions per 100
12.49 (Fixed)
103.1 (Mobile)

Broadband Subscriptions per 100
Fixed 2.65
Wireless 7.8

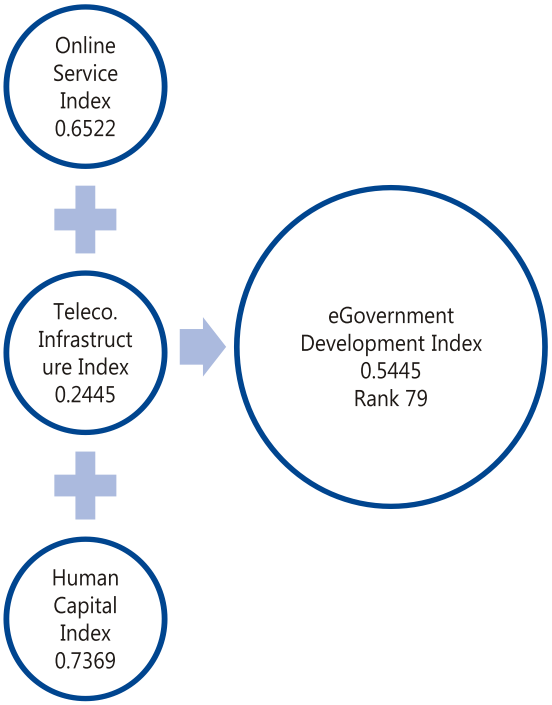
Internet Usage
21.3%
Email usage
11%

a. Computer Literacy 28.3%
(Urban 41.1%, Rural 26.5%, Estate 9.5%)
b. Digital Literacy 38.7%
(Urban 54.5%, Rural 36.4%, Estate 16.4%)

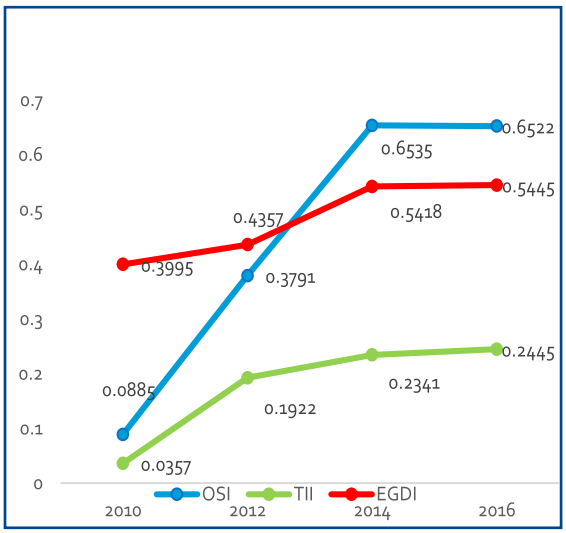
Devices use to Connect to Internet
Desktop or Laptops 38.1%
Smart Phones 56.9%
Tablets 2.1%
Mobile Phones 2.9%

Our Progress in Digital Government

Sri Lanka is ranked 79 in the United Nations e-government development index (EGDI) among 190 member countries[4]. In 2016, we scored (a) 0.6522 in online service index (OSI) which focuses on overall digital government applications, (b) 0.2445 in telecommunication infrastructure index (TII) which focuses on the status of telecommunication infrastructure, Internet facilities, and Internet usage, and (c) 0.7363 human capital index (HCI) which focus on adult literacy and level of schooling[4]. Thus, our scores in the online service index and the human capital index are above the global average while our score in the telecommunication infrastructure index is below the global average.



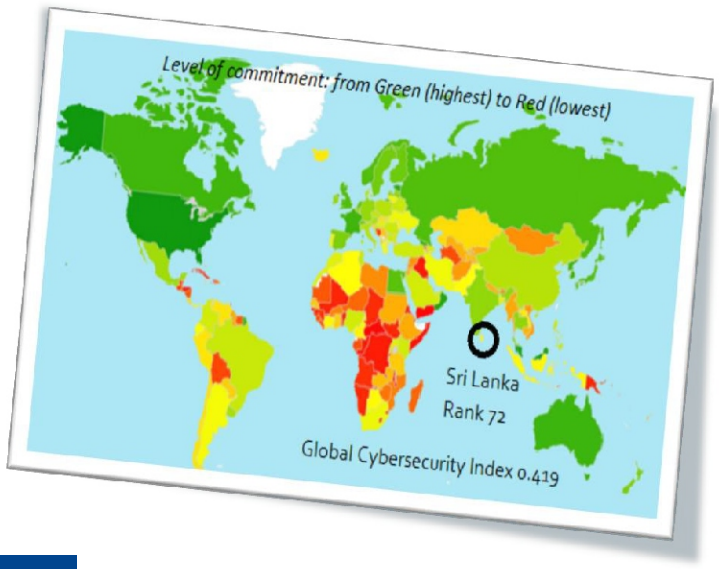
Progress of the development of digital government[5]



Cyber Security Landscape

Our Status in the Cybersecurity Index

Among the 193 ITU member countries, Sri Lanka is ranked 72 in the Global Cybersecurity Index (GCI) in the year 2016[6]. GCI assesses a country's overall commitment towards cyber security in relation to five different dimensions, namely (a) legal, (b) technical, (c) capacity building, (d) organizational, and (e) cooperation dimensions[6]. Our performance in each dimension is assessed and rated either as initiating, maturing, or leading. Sri Lanka's overall performance is rated as maturing.



Our Performance in the GCI[6] (2017)

a. LEGAL: We are Initiating
Assessed with reference to the existence of legislation on cybercrime and cyber security, and legal training.

b. TECHNICAL: We are Maturing
Assessed with reference to the existence of technical institutions and frameworks for dealing with cybersecurity related issues.

c. CAPACITY BUILDING: We are Maturing
Measured based on the existence of research and development, education and training programs, certified professionals and public sector agencies fostering capacity building

d. ORGANIZATIONAL: We are Maturing
Assessed based on the existence of institutions for policy formulation and coordination, and strategies for cybersecurity development at the national level

e. COOPERATION: We are Initiating
Measured based on the existence of partnerships, cooperative frameworks and information sharing networks

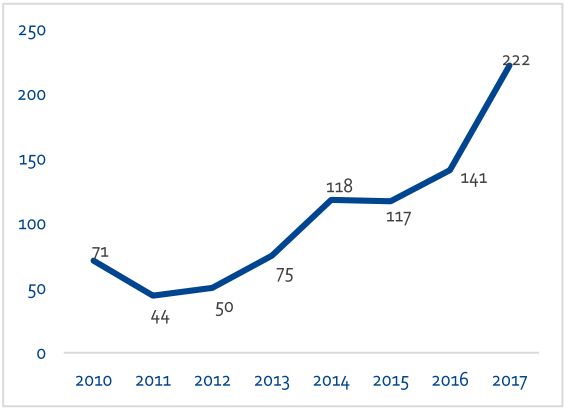
Our Performance in the GCI in detail[6]

Assessment Criteria	*Assessment Sub Criteria*	*Our Status*
a. Legal	*Cyber Crime Legislation*	*Initiating*
	Cyber Security Legislation	*Initiating*
	Cyber Security Trainings	*Leading*
b. Technical	*National CERT/CIRT/CSIRT*	*Leading*
	Government CERT/CSIRT	*Leading*
	Sectoral CERT/CIRT/CSIRT	*Leading*
	Standards for Organizations	*Initiating*
	Standards for Professionals	*Initiating*
	Child Online Protection	*Initiating*
c. Capacity Building	*Standardization bodies*	*Initiating*
	Cybersecurity good practices	*Leading*
	R & D Programs	*Maturing*
	Public awareness campaigns	*Leading*
	Professional training courses	*Leading*
	Educational programs	*Maturing*
	Incentive mechanisms	*Initiating*
	Home-grown industry	*Initiating*
d. Organizational	*Strategy*	*Initiating*
	Responsible Agency	*Maturing*
	Cyber Security Metrics	*Initiating*
e. Cooperation	*Bilateral agreements*	*Initiating*
	Multilateral agreements	*Leading*
	International participation	*Leading*
	Public-private partnerships	*Maturing*
	Interagency partnerships	*Initiating*

Incidents Reported

Over the past few years, Sri Lanka CERT|CC has experienced a rapid increase in the number of cybersecurity related incidents reported to it. Reported incidents rose from 71 to 222 from 2010 to 2017. The number of reported social media related incidents, have also increased exponentially. It has ballooned from 80 incidents in 2010 to 3685 incidents in 2017.

Growth in Cybersecurity related incidents



Incidents Types	2012	2013	2014	2015	2016	2017
Phishing	08	08	12	14	23	42
Privacy Violation	08	08	08	21	32	29
Scams	06	18	12	18	12	32
Malicious Software/ Ransomware	02	02	03	12	21	39
Financial Frauds	-	-	-	10	16	35
Compromise Websites	15	16	56	20	10	25
Compromise Emails	06	08	10	16	16	14
Intellectual Property Violation	03	03	03	03	07	06
Unauthorized Access	01	11	08	-	-	-
DoS/DDoS	01	01	06	03	04	-
Social Media Incidents	1100	1200	2250	2850	2200	3685

FAST FACTS ON SOCIAL MEDIA RELATED INCIDENTS (2017)

4.2 million

Use Facebook in Sri Lanka. This amounts to 63% of the total number of Internet users in Sri Lanka[7].

Some facts as reported to Sri Lanka CERT|CC *2017*

3685 Social Media Related Incidents Reported

2018 Fake Social Media Accounts
829 Incidents of Hacking Social Media Accounts

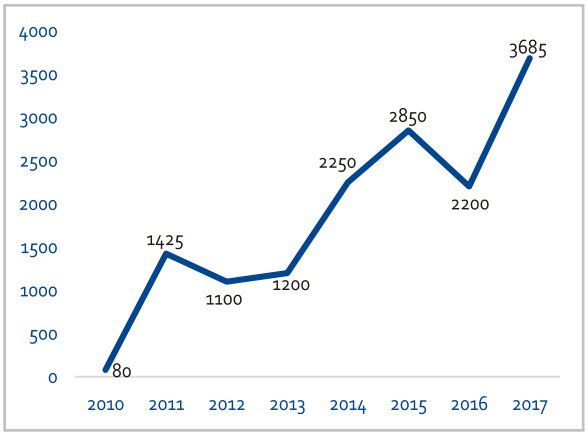
416 Incidents on Photo Abuse

57 Incidents on Threatening and Cyberbullying
54 Incidents on Misuse of Phone Numbers

17 Incidents on Pornographic Videos
7 Copyright Violations

Other 287

Growth in Social media related incidents



Our Strategy

Our vision *is to create a resilient and trusted cyber security ecosystem that will enable Sri Lankan citizens to realize the benefits of digitalization and to facilitate growth*

Six Strategic Thrust Areas

1. **Establishment of Governance Framework**
   Establishment of a governance framework to implement National Information and Cyber Security Strategy

2. **Enactment and Establishment of Legislation, Policies and Standards**
   Formulation of legislation, policies, and standards to create a regulatory environment to protect individuals and organizations in the cyber space

3. **Development of Competent Workforce**
   Development of a skilled and competent workforce to detect, defend and respond to cyber-attacks

4. **Resilient Digital Government and Infrastructure**
   Work with public sector authorities to ensure that the digital government systems implemented and operated by them have the appropriate level of cyber security and resilience

5. **Raising Awareness and Empowerment of Citizens**
   Make our citizens more competent in protecting their identity, privacy and economic assets in the cyber space

6. **Development of Public-Private, Local-International Partnerships**
   Development of public-private, local-international partnerships to create a robust cybersecurity ecosystem

Thrust # 1: Establishment of the Governance Framework

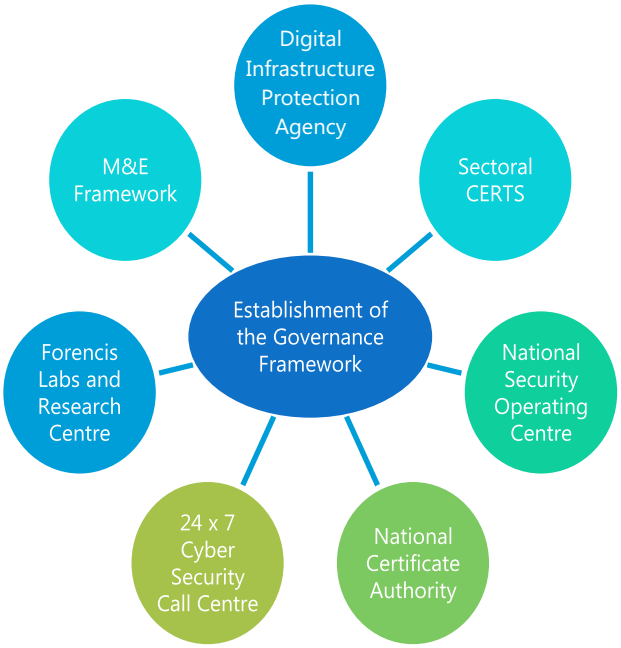
Our Strategy

In 2006, the government of Sri Lanka established Sri Lanka CERT|CC as the single trusted source of advice on the latest threats and vulnerabilities affecting computer systems and networks, charged with the responsibility of providing technical support in responding to and recovering from cyber-attacks. Sri Lanka CERT was established under the Information and Communication Technology Agency (ICTA) of Sri Lanka, and now it is operating directly under the purview of the Ministry of Telecommunication, Digital Infrastructure and Foreign Employment.

As the complexity of the cyber security ecosystem increases, the government of Sri Lanka recognizes the necessity of introducing a National Information and Cyber Security Strategy to cope with emerging threats. It is a high-level top-down approach to information and cyber security that establishes a range of national objectives and priorities that should be achieved in a specific timeframe.

In line with the strategy, a Digital Infrastructure Protection Agency will be established. The Agency will be responsible for overseeing the implementation of the cyber security strategy, setting national polices, facilitating the protection of critical national infrastructure, educating citizens, building a pioneering technology competent workforce, and promoting industry development.

Our strategy *is to establish a powerful agency which oversees the overall implementation of the Information and Cyber Security Strategy of Sri Lanka, and to establish specialized subordinate agencies for effectively battling emerging cyber threats*



Our Initiatives

1.1. Establishment of the Digital Infrastructure Protection Agency (DIPA) of Sri Lanka

DIPA will be established as the apex institution for all cyber security related affairs in Sri Lanka. The Agency mandate shall be to oversee the implementation of the National Information and Cyber Security Strategy.

The agency shall,

1.1.1 Function as the command and control body to promote this strategy and play a leading role in implementing cyber security initiatives set forth in this strategy.

1.1.2. Provide technical support for law enforcement authorities in conducting digital forensic investigations.

1.1.3. Build the capacity of sectoral CERTs and facilitate Sri Lanka CERT|CC to coordinate with sectoral CERTs for sharing incident information, best practices and other security related information.

1.1.4. Provide technical support to government bodies such as Ministries, authorities, boards, corporations etc.

1.1.5. Disseminate emerging cyber threat warnings to all Sri Lankans.

1.1.6. Act as a certification body issuing licenses for firms providing information security related services.

1.2. Institutions Under the DIPA

1.2.1. Sri Lanka CERT|CC will continue to operate as the National CERT to protect users in the public and private sector organizations and the general public by providing up-to-date information on potential threats and vulnerabilities, and by undertaking computer emergency response handling services.

1.2.2. DIPA will establish a 24 X 7 Cyber Security Call Centre with a focus on assisting citizens, government organizations, and private firms to respond to cyber security incidents.

1.2.3. DIPA will establish a National Cyber Alert System with the involvement of Internet Service Providers (ISPs) and Telcos to deliver targeted, timely, and actionable information to Sri Lankans and to educate citizens on how to secure their computer systems.

1.2.4. DIPA will establish a Digital Forensic Lab to conduct digital forensic investigations and examinations in the areas of computer forensics, mobile forensics, audio forensics, video forensics and so forth.

1.2.5. DIPA will establish the National Cyber Security Operating Centre (NCSOC) for monitoring threats to digital government applications, critical information infrastructure, and critical systems of private firms.

1.2.6. DIPA will establish the National Certification Authority (NCA) to address the limitations of the Certification Service Providers (CSPs).

DIPA will establish a Research Unit for developing, coordinating and stimulating continuous research activities in the fields of Strategic Policy Research, Information Security Research, Cyber Security and Technology related research.

1.3. Monitoring and Evaluation (M&E) Framework

A comprehensive results based M&E framework will be developed to assess and measure the performance of the outcomes and outputs as a result of the implementation of the strategy.

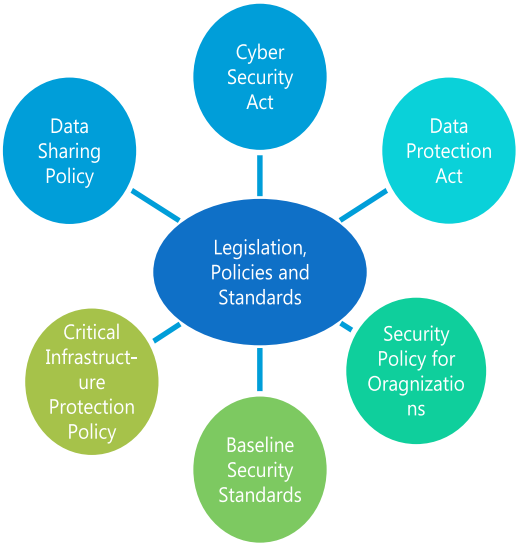
Thrust # 2: Legislation, Polices, and Standards

Our Strategy

The number of reported incidents involving cybercrimes against individuals and organization in Sri Lanka is increasing day by day. These include cybercrimes against individuals such as credit card fraud, revenge porn, crimes again property such as worm attacks, hacking, and intellectual property theft, and crimes against governmental and other organizations such as cyber terrorism, hacking of websites, processing of unauthorized information, and hacking into sensitive financial data. To battle cybercrimes against individuals and organizations effectively, it is necessary to enact and formulate appropriate legislation, policies, and standards for ensuring protection of sensitive data, digital transactions, electronic communications, privacy, and freedom of expression in the cyber space.

The government of Sri Lanka has taken a number of steps in this regard such as the introduction of the government security policy (2009) based on ISO 27000, and data sharing policy, and the enactment of relevant legislation such as the Electronic Transactions Act No. 19 of 2006, Payment Devices Frauds Act No 30 of 2006, the Intellectual Property Rights Acts, and Computer Crimes Act No 24 of 2007. Sri Lanka ratified the Budapest Convention on Cybercrime in 2015 and became the first country in South Asia to join this convention. Moreover, a Computer Crimes Division was established in the Criminal Investigation Department of Sri Lanka Police in line with the enactment of Computer Crimes Act.

To further strengthen our regulatory framework to effectively battle emerging cybercrimes, gaps in the existing policies and laws will be identified, and new legislation, policies, and standards will be drafted and implemented to create a secure cyberspace for individuals and organizations.



Our strategy *is to create an appropriate regulatory framework for securing individuals and organizations in the cyberspace and to strengthen prosecution support for modern cyber offences through the introduction of relevant legislation, policies and standards*

Our Initiatives

2.1. Introduce a New Cyber Security Act

2.1.1. The government will introduce a new Cybersecurity Act for the establishment of the DIPA and for equipping the agency with the necessary powers to effectively address increasingly sophisticated threats to the nation

2.1.2. The new Act will establish a comprehensive framework for the prevention and management of Cyber Security threats and incidents effectively, and protection of critical information infrastructure.

2.2. Data Protection and Privacy Laws

2.2.1. Currently, the number of cases on stealing customer data is on the rise. However, Sri Lanka lacks appropriate laws to protect customer data. We will, therefore, introduce a data privacy and protection law which governs the collection, use, and disclosure of citizens' personal data by government and private sector organizations.

2.2.2. Through this act, we will ensure that all government organizations and private sector firms which maintain citizens' data have adequate security controls in place and make them liable for privacy violations.

2.3. Data Sharing Policy

2.3.1. We will also introduce a data sharing policy for government organizations

2.4. Baseline Security Standards

We will facilitate the Sri Lanka Standards Institute to develop baseline information and cyber security standards for information systems, hardware, and software applications.

2.5. Critical Infrastructure Protection Policy

We will introduce Critical Infrastructure Protection Policy which will identify and declare infrastructure as critical infrastructure and provide measures necessary for protecting, safeguarding and increasing resilience of critical infrastructure.

2.6. Information Security Policy

We will facilitate organizations to develop security policies based on the maturity of their information systems. The information security policy of each organization shall be developed aligning with international standards.

Thrust # 3: Development of a Competent Workforce

Our Strategy

Cyber-attacks and the disruptions to information systems caused by these attacks are increasing exponentially. In this context, it is necessary to ensure the availability of a cadre of knowledgeable and highly skilled professionals in the field of information and cyber security domain to protect, detect, defend and respond to these cyber-attacks.

In 2016, skills gap analysis from ISACA estimated a global shortage of 2 million cybersecurity professionals by 2019[8]. As per the GCI, Sri Lanka requires to expend much effort on building overall human resource capacity to combat emerging cyber threats. In Sri Lanka, to date, there is a distinct lack of initiatives to address the domestic shortage of cybersecurity experts. We will, therefore, aim to implement appropriate strategies to facilitate our workforce to gain and maintain the knowledge, skills, experience and technological capabilities needed to effectively work in the cyber environment.

Our strategy is *to create a virtuous circle of supply and demand of information and cyber security experts through continuous assessment of the gap between the supply and demand of cyber professionals, increasing learning opportunities to capitalize on cyber security knowledge, and educating youth for building a pool of future cybersecurity professionals*

Our Initiatives

3.1. Assess Supply and Demand of Professionals

We will conduct a national level survey to understand the gap between the supply of information and cybersecurity professionals and demand from the industry for such professionals in Sri Lanka. Such an analysis is important for DIPA to formulate appropriate strategies and policies to fill the supply and demand gap.

3.2. Competency Framework

3.2.1. We will develop a National Information and Cyber Security Competency Framework which outlines the core competencies that both the government and private sector should possess to effectively work in the cyber environment. In developing the framework, carder structure of the public service and private sector would be taken into account.

3.2.2. We will work with Tertiary and Vocational Education Commission to develop National Vocational Qualification (NVQ) standards for various disciplines in the Information and Cyber Security domain. The proposed National Information and Cyber Security Competency Framework shall comply with the NVQ Standards and Professional Qualification Standards as defined by International Standardization bodies.

3.3. Up-Skilling and Re-Skilling Opportunities for Public Sector Staff

A minimum NVQ standard will be introduced as a qualification requirement for each layer of staff in the Information Technology service, and in other services who are involved with ICT initiatives.

3.3.1. We will also facilitate the organizing of special training courses (based on NVQ Standards) for the staff of agencies maintaining critical infrastructure, agencies dealing with most vulnerable communities in our society, law enforcement authorities, Tri-forces and the Intelligence Services.

3.3.2. As per Information and Cyber Security Competency Framework, we will roll out information and cyber security training program for staff at grass root level organizations in the public service across the country.

3.3.3. We will offer scholarships for public sector staff to undertake specialized postgraduate degrees and to take up professional courses in this domain.

3.3.4. We will include information and cyber security for Confidence and Efficiency Bar exams in public service.

3.4. Expanding Tertiary and Vocational Education

3.4.1. We will facilitate local universities, vocational training institutes, and private educational service providers to introduce industry oriented diplomas, undergraduate and post graduate programs to provide learning opportunities to students to develop a solid foundation in both theory and practice of information security to advance their practical cybersecurity skills.

3.4.2. We will facilitate private professional entities/accreditation institutes to award professional qualifications in this domain.

3.5. Training Infrastructure across the Country

3.5.1. We will facilitate private firms to develop information and cyber security training infrastructure across the country by way of public private partnership arrangements.

3.5.2. We will empower government training institutes (e.g. Sri Lanka Institute of Development Administration, Sri Lanka Institute of Local Governance) to conduct information and cyber security training for government staff.

3.6. e-Learning Modules

We will encourage the Distance Learning Centre to design e-learning modules on Cyber Security which government staff can take up upon their convenience.

3.7. Opportunities for Government Staff to Attend International Conferences

Continuous participation and contribution to international conferences on information security is essential to state our position and deepen communications with various actors around the world. We recognize that participation at such conferences would not only help to capitalize on cybersecurity expertise knowledge but also to build networks with cyber security professionals from around the globe. Through our international partnerships and the External Resource Department of Sri Lanka, we will seek such opportunities for Chief Innovation Officers (CIOs) and Chief Information Security Officers of the public service.

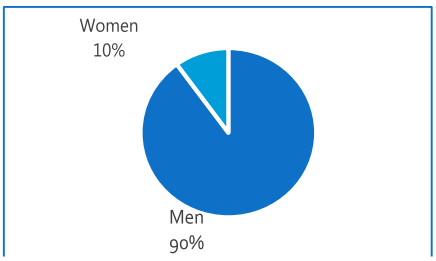
3.8. Future Career Paths

3.8.1. We will advocate for inclusion of information and cyber security into the school curriculum with the aim of creating a talented pool of cyber security professionals in future.

3.8.2. We will facilitate career guidance workshops at schools across the country to raise awareness of the emerging career opportunities in this domain. Students who are completing GCE A/L shall be the target group.

3.8.3. Women are globally underrepresented in the cybersecurity profession. Globally it is at 11%, much lower than the representation of women in the overall global workforce Special attention will be given to creating an interest in cybersecurity among female school students as there is inadequate women participation in this domain.

Women in Cybersecurity Workforce (Asia Pacific Region)[10]



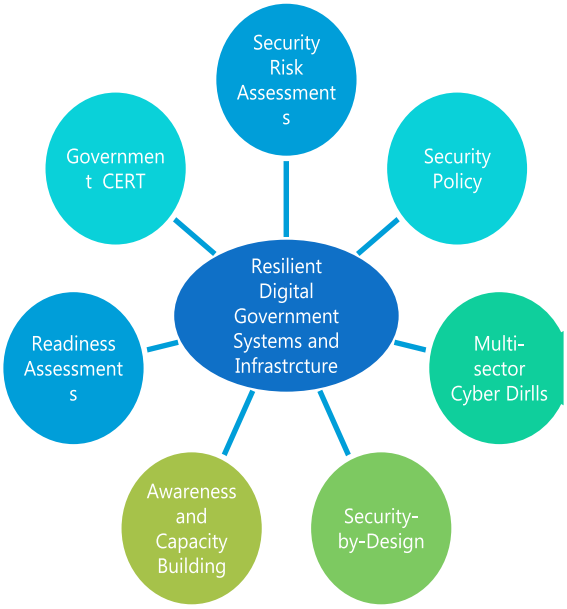
Thrust # 4: Resilient Digital Government Systems and Infrastructure

Our Strategy

Sri Lanka has advanced rapidly over the past decade in developing various digital government initiatives. Multimillion investments made on various digital government initiatives have helped Sri Lanka to advance from 101st (2008) to 79th position (2016) in the e-Government Development Index[4]. To date there are about 500 government websites and more than 50 e-services facilitating citizens to obtain services through the Internet. e-Administrative applications have been developed by public organizations that maintain critical infrastructure with the aim of increasing the organizational efficiency thereby providing better services for citizens. Lanka Government Network, and Lanka Government Cloud provide the necessary digital infrastructure for e-services and e-administrative services.

Although digital government initiatives promise tremendous benefits for citizens and government, they also bring threats of various cyberattacks such as malware attacks, unauthorized access, and denial of service attacks. Cyber-attacks on digital government services can cause significant disruptions to the public service delivery, and thereby destroy public confidence. Our citizens will not embrace digital government if their information cannot be securely kept in the government systems. It is, therefore, essential to adopt appropriate strategies to ensure security of digital government systems and critical information infrastructure.

Our strategy *is to ensure that our digital systems and digital infrastructure are resilient to cyber threats, through implementing risk management processes, implementing appropriate security policies and strategies at the organizational level, increasing awareness and building the capacity of public sector staff at all levels*



Our Initiatives

4.1. **Information and Cyber Security Risk Assessments**

4.1.1. We will conduct a survey to identify the organizations (both private and public) which maintain critical information systems. An inventory of organizations shall be developed based on the criticality of the information infrastructure maintained by the relevant organization.

4.1.2. We will facilitate relevant stakeholders to conduct information and cyber security risk assessments to uncover weaknesses and vulnerabilities in digital government systems and infrastructure, and to prioritize and implement appropriate security controls to mitigate those identified weaknesses.

4.2. Security Policy for Organizations that Maintain Digital Government Systems

We will facilitate the organizations maintaining digital government systems and organizations maintaining critical infrastructure to develop and implement the Information Security Policy based on international standards.

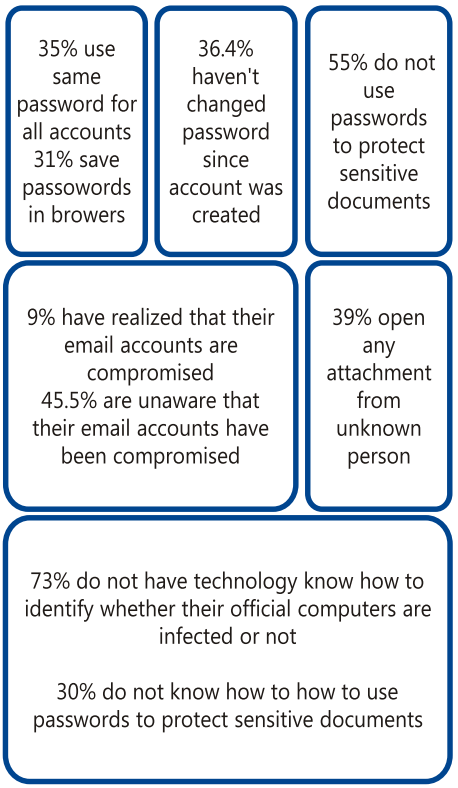
4.3. Digital Government Infrastructure Protection Unit

4.3.1. To effectively defend the digital government systems and infrastructure from emerging threats, we will setup the Digital Government Infrastructure Protection Unit under DIPA. This unit will be responsible for detecting and analyzing cyber threats and vulnerabilities, disseminating cyber threat alerts, and coordinating incident response activities.

4.3.2. We will coordinate multi-sector cybersecurity exercises with the involvement of this unit. Through these exercises, we aim to identify vulnerabilities arising from cross-sector interdependencies and stress-test coordination and communication across sectors.

4.4. Awareness and Capacity Building of Staff Working with Digital Government

Some facts (2017)



4.4.1. It is widely believed that the awareness of Sri Lankan public officers on information and cyber security should be improved. We will, therefore, first conduct information and cyber security readiness surveys on public sector employees periodically to assess their readiness to work in a digital government environment.

4.4.2. In line with the Competency Framework, CIOs and Technical staff working in digital government environment will be empowered with appropriate skills and knowledge on information and cyber security.

4.4.3. As per the Information and Cyber Security Competency Framework (Thrust Area 3), we will, conduct information and cyber security awareness activities across all levels of government staff.

4.5. Chief Information Security Officer and Information Security Officers

4.5.1. We will work with the Department of Management Service to establish a "Chief Information Security Officer" position in the public service, which will be the highest level position in the information and cyber security domain in the public service.

4.5.2. Depending on the usage of ICT systems at public organizations, we will appoint Information Security Officers for government organizations and develop their capacity through comprehensive knowledge building exercises.

4.6. Security-by-Design in Digital Government Systems Development

4.6.1. Security-by-Design is a best practice which can be adopted to secure digital government upfront and throughout its life cycle. By integrating risk assessment into the system development life cycle, trade-offs between security, cost and functionalities can be balanced. We will encourage solution developers to incorporate security-by-design principles when developing digital government systems and digital infrastructure.

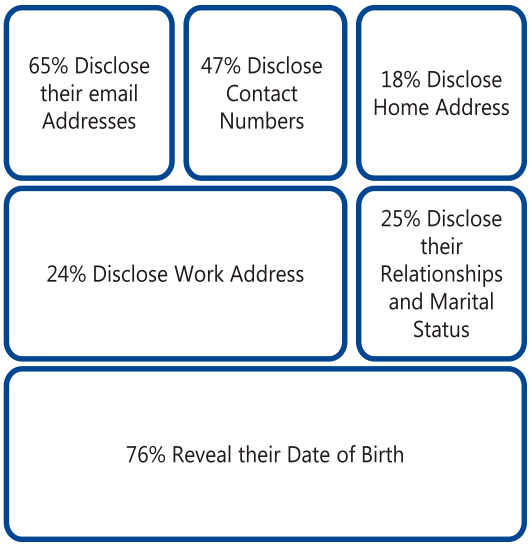
4.6.2. We will work with the National Procurement Commission of Sri Lanka to incorporate such conditions to standard government bidding documents.

Thrust # 5: Raising Awareness and Empowerment of Citizens

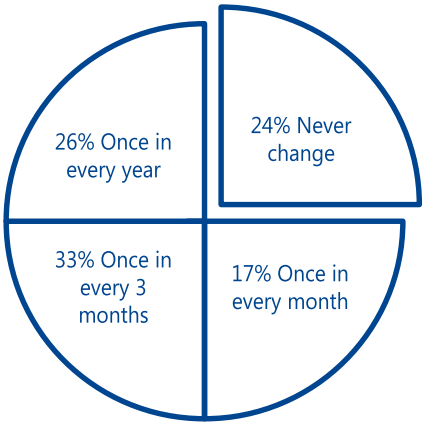
Our Strategy

The Internet has become important for all aspects of daily life including education, work, and participation in society. A considerable segment of society is becoming more and more dependent on the Internet thereby becoming more vulnerable to cybercrime. A major reason for such vulnerabilities to cybercrime is lack of awareness among citizens about possible cyber threats and their consequences. Theft of identity, stealing of credit card numbers, and privacy violation and unauthorized access on social media for example are commonly caused due to the lack of awareness of citizens. It is, therefore, essential to raise citizens' awareness about emerging cyber threats and empower them with the knowledge and skills necessary to defend themselves against evolving cyber threats.

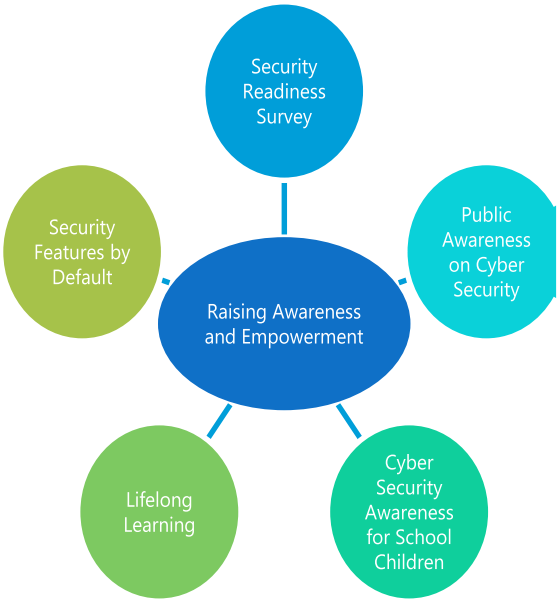
Some facts on the disclosure of identity and privacy by Sri Lankan youth through social media



Frequency of changing the password of social media by Sri Lankan youth



***Our strategy is** to raise the awareness of citizens about the risks derived from cyberspace, and build their capacity to protect their identity, privacy and economic assets in the cyber space*



Our Initiatives

5.1. National Information and Cyber Security Readiness Survey

In collaboration with the Department of Census and Statistics, we will conduct a National Baseline Survey to assess Sri Lankan citizens' awareness, attitudes and behaviors on cyber security related activities.

5.2. Public's Awareness of Social Media and Cyber Security

5.2.1. We will extend the services of CERT website to provide a comprehensive collection of materials and activities relating to cybersecurity, and incorporate a comprehensive complaints reporting system to assist victims.

5.2.2. We will increase information and cyber security awareness among the public through hosting awareness campaigns, organizing public conferences, street dramas, and so forth.

5.2.3. We will pay special attention to most vulnerable communities in the society including youth, women and elderly people.

5.2.4. We will use printed and electronic media to reach a broader population. Content shall be in trilingual format. We will also use social media as a tool for increasing the information security awareness of citizens.

5.2.5. We will also enhance the content of well-known government web sites (e.g. www.gov.lk,www.news.gov.lk, www. defence.gov.lk) with information and cyber security related materials (e.g. presentations, and webinars). The Government Call Centre (1919) will be also enhanced to provide basic information on cyber security related matters.

5.3. Introduction of Information and Cyber Security into Curriculums

5.3.1. We will facilitate the Ministry of Education and the National Institute of Education to include information and cyber security as an essential part of the informatics curriculum at schools.

5.3.2. We will facilitate the Ministry of Education to increase school children's awareness on cyber security. We will also continue to publish the Cyber Guardian (newsletter on cybersecurity) and circulate among school and university students to increase their awareness on latest cyber threats.

5.4. Lifelong Learning Opportunities

With the involvement of Open University of Sri Lanka and Vocational Training Institutes we will design basic information and cyber security learning modules for adults. We aim to deliver these courses through the Open University's distance learning centres, Nenasala Centres, vocational training institutes and accredited training institutes scattered around country.

5.5. Security Ratings for ICT Equipment and Create Awareness Among Citizens

We will facilitate the Sri Lanka Standards Institute to develop Security Ratings for ICT products which will enable citizens to have a clear idea of the level of security that a product offers. We will also work with ICT product suppliers' associations to supply products into the market by enabling security settings by default. Through effective communication channels we will make citizens aware of security ratings and security features of ICT products.

Thrust # 6: Development of Public-Private, Local-International Partnerships

Our Strategy

Sri Lankan cyber community as a part of the global Internet community faces many vulnerabilities. Social engineered Trojans attacks, malware attacks, phishing attacks, advanced persistent threats, botnets, ransomware, financial frauds for example are increasingly posing many threats to the Sri Lankan Internet community.

The government of Sri Lanka acknowledges that the government alone cannot effectively combat these threats. Collective efforts of end users, academics, private sector hardware and software vendors, Telcos and ISPs, private sector critical infrastructure owners, are essential in battling against these cyber threats. Moreover, cybersecurity cannot be achieved by any one nation alone, and greater levels of international cooperation is needed to confront those actors who seek to disrupt or exploit our networks.

Our strategy *is to develop a mechanism for cooperation extending beyond government agencies to public-private collaboration, and local- international collaboration in developing a cybersecurity ecosystem*

Our Initiatives

6.1. Partner with Telecommunication and ISPs to Protect Internet Users

6.1.1. ISPs in Sri Lanka occupy a unique position as the gateway to Sri Lanka's cyberspace. We will, therefore, set up a Telco-CERT with the involvement of Telcos and ISPs to effectively handle emerging cyber threats. Telco-CERT would be involved in tackling phishing attacks, blocking malicious domains and IP addresses, and deploying other measures to disrupt malware attacks including measures to secure the telecommunications and Internet routing infrastructure.

6.1.2. We will encourage ISPs to increase their customers' awareness on cyber security risks, and best practices for avoiding cyber threats.

6.2. IP Reputational Service

We will work with Telecommunication Regulatory Authority of Sri Lanka (TRC) and ISPs to determine the possibility of maintaining an Internet Protocol Reputation Service. This will facilitate online service providers to obtain information about an IP address to which they are connecting. Through this service, spreading of harmful content shall be minimized.

6.3. Partner with Firms Operating Critical Information Infrastructure (CII) to Create Resilience

Our systems depend on the critical infrastructure information systems that are owned by non-government actors. There are many private companies which provide critical services to the general public in the domains of finance, power and energy, transport, aviation, health and so forth. Although the government is not responsible for securing the critical information infrastructure owned by private firms, it is essential to support these private firms to protect their information infrastructure where a damage to the information infrastructure would interrupt the day-to-day lives of citizens. We will therefore, work closely with Critical Infrastructure owners and operators to expand initiatives to secure the CII ecosystem, preserve the benefits of cyberspace, and avoid unnecessary impediments to technological evolution.

6.4. Empower Sectoral Ministries Maintaining Digital Government Systems

The primary responsibility of safeguarding security in each sector's digital government systems and infrastructure, and of ensuring adequate preventive measures against cyber threats lies with the sectoral ministries. This means that each sectoral ministry has a responsibility of identifying critical infrastructure in their sector, and ensuring

adequate security by assessing, determining and implementing preventive measures in their sector.

6.5. Work with Military Establishments to Establish a Joint Military Security Operation Centre/Defence CERT

Sri Lankan Militaries, Police, and Intelligence Services all work separately in confronting malicious cyber actors. However, there is a lack of coordination among these organizations to share valuable information on cyber threats. In this context, with the involvement of relevant authorities, we will establish a joint Cyber Security Operations Centre/Defence CERT with a focus on strengthening our cyber defences and ensuring that our defence forces are able to continue to operate securely. The creation of a single unified military security operations centre would provide better capabilities to speedily overcome challenges presented by operating in cyberspace.

6.6. Promote Cooperation with Industry Sectors

6.6.1. We will encourage industry sectors to work together in order to jointly improve detection, prevention, response and recovery capabilities.

6.6.2. We will develop a channel to share real-time sensitive information on cyber threats and potential consequences with industry sectors. We will also develop a mechanism to share information on cyber threats and vulnerabilities with medium size businesses, which are currently increasingly being victimized by malicious actors in the cyber space. Tailored alerts and advice will be generated for them.

6.7. Strengthening International Partnerships

Through effective operational links between countries and across the region, we will engage with the international community to build a system of cyberspace stability. We will sign agreements with international organizations such as International Telecommunication Union (ITU), The European Union Agency for Network and Information Security (ENISA), Asia Pacific Computer Emergency Response Team (APCERT), Internet Corporation for Assigned Names and Numbers (ICANN), Forum for Incident Response Security Teams (FIRST), United Nations Internet Governance Forum (UNIGF), Internet Society (ISOC), International Watch and Warning Network (IWWN), and the International Criminal Police Organization (Interpol) for exchanging technical information on threats and vulnerabilities, obtaining latest software and hardware products, conducting joint cyber drills, and building the capacity of the staff.

6.8. Budapest Convention

On 1st September 2015, Sri Lanka ratified the Council of Europe's Convention on Cybercrime (Budapest Convention) and became the first country in South Asia to become a party to the Convention. The Budapest Convention is the only international legally binding treaty on Cybercrime in the world today and seeks to harmonize national laws, adopt improved investigative powers based on international standards, enhance criminal justice cooperation among State Parties in order to effectively combat the threat against cybercrime [9]. We will take initiatives to implement and comply with the Budapest Convention requirements and will continuously work with member countries to build a secure cyber space.

6.9. Increase our Presence at International Level

We will enhance our presence at the international level through participation in international forums and conferences on cyber security and through playing an active role in knowledge gaining and sharing exercises.

6.10. Partner with Businesses to Promote Security in Products and Services

We will work with suppliers to bring products and services to the market with a high level of security to ensure the privacy and security of customer information.

6.11. Partner with Universities to build a Cyber Security Research Culture

6.11.1. We will work with Universities in Sri Lanka to promote a cybersecurity research culture in Sri Lanka.

6.11.2. In partnership with donors and universities, we will introduce research grant schemes for students undertaking research on cyber security.

6.11.3. With the partnership of all stakeholders in this domain we will continue to host an annual national cybersecurity week followed by a national cyber security conference.

6.12. Support of Government Organizations, Social Groups and NGOs

6.12.1. With the involvement of government stakeholders including the Ministry of Social Empowerment and Welfare, Ministry of Women and Child Affairs, the Child Protection Authority, and Ministry of Law and Order we will increase the awareness of rural communities, and most vulnerable communities in our society on cyber security.

6.12.2. With the involvement of groups in the civil society (e.g. SMART Social Circles, Nenasala Centres, Community Centres), and NGOs, we will increase rural and semi urban citizens' awareness on cyber security, and help and guide citizens towards safe, enjoyable experiences online.

6.13. Nurture Start-ups

We aim to support entrepreneurs to establish cyber security startups. We will nurture start-ups to boost the development of niche solutions and grow local champions to sustain strategic areas of interest. In partnerships with Sri Lanka Software Exporters Association, we will develop market opportunities to bring made-in-Sri Lanka solutions into the global market.

End Notes

1. https://www.statista.com/statistics/387857/number-cyber-security-incidents-worldwide/
2. https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion
3. http://www.statistics.gov.lk/education/ComputerLiteracy/ComputerLiteracy-2017Q1-Q2-final.pdf
4. http://workspace.unpan.org/sites/Internet/Documents/UNPAN96407.pdf
5. https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2010
6. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
7. http://www.internetworldstats.com/stats3.htm
8. https://image-store.slidesharecdn.com/be4eaf1a-eea6-4b97-b36e-b62dfc8dcbae-original.jpeg
9. https://rm.coe.int/16806bdcd8
10. https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf

Notes

Sri Lanka CERT | CC

Room 4-112, BMICH,
Bauddhaloka Mawatha, Colombo 07, Sri Lanka.
Tel: +94 11 269 1692 / 269 5749 / 267 9888
Fax: +94 11 2691064
E-mail: cert@cert.gov.lk

www.cert.gov.lk