Annual Activity Report 2020

Sri Lanka CERT | CC

The National CERT of Sri Lanka

CONTENTS

ABOUT SRI LANKA CERT|CC

INTRODUCTION

The Sri Lanka Computer Emergency Readiness Team | Coordination Centre (Sri Lanka CERT|CC) is the National Centre for cyber security in Sri Lanka, mandated to protect Sri Lanka's Information and Information Systems Infrastructure. Its services range from responding to investigating information security breaches, in order to prevent security breaches through awareness, security assessments, Managed services, Forensics and capability building.

ESTABLISHMENT

As the National CERT of Sri Lanka, Sri Lanka CERT acts as the focal point for cyber security of the nation. It is the single trusted source of advice about the latest threats and vulnerabilities affecting computer systems and networks, and a source of expertise to assist the nation and member organizations, in responding to and recovering from Cyber-attacks.

Sri Lanka CERT was established on 1st of July 2006 as a subsidiary of Information and Communication Technology Agency of Sri Lanka (ICTA). Currently Sri Lanka CERT functions under the purview of Ministry of Technology.

WORKFORCE

At the end of 2020, the Sri Lanka CERT team comprised of twenty-three (23) staff members. This includes the Chief Executive Officer, Chief Operating Officer, Head of Research, Policy and Projects, Chief Information Security Engineer, three Information Security Engineers, five Associate Information Security Engineers, two project managers, four Information Security Analysts, two Associate Information Security Analysts, Head of Human Resources and Administration, Admin & Account Assistant and a driver cum office assistant. In addition, there are six undergraduate interns assisting the operation of the organizations. Eight staff members were recruited during the year 2020. During the period, six undergraduate interns completed their internships at the organization (June 2020).

All the staff are highly skilled and experienced in different areas of information security and have achieved corresponding Information Security certifications which are widely recognized in the industry, such as SANS GCIH, Microsoft MCSE, EC-Council CEH and CHFI, Red Hat RHCSA, RHCE, Cisco CCNA and CCSP and CISSP by International Information Systems Security Certification Consortium; (ISC)².

CONSTITUENCY

Sri Lanka CERT 's Constituency encompasses the whole of the cyber community of Sri Lanka (private & public sector organizations, and the general public). Sri Lanka CERT maintains a good rapport with government and private sector establishments, and extends assistance to the general public as permitted by available resources. In accordance with its mandate, Sri Lanka CERT | CC gives priority to requests for assistance from government agencies. Based on availability of human resources and necessary skills, requests from private sector are handled free of charge or on a paid basis, depending on the type of service provided.

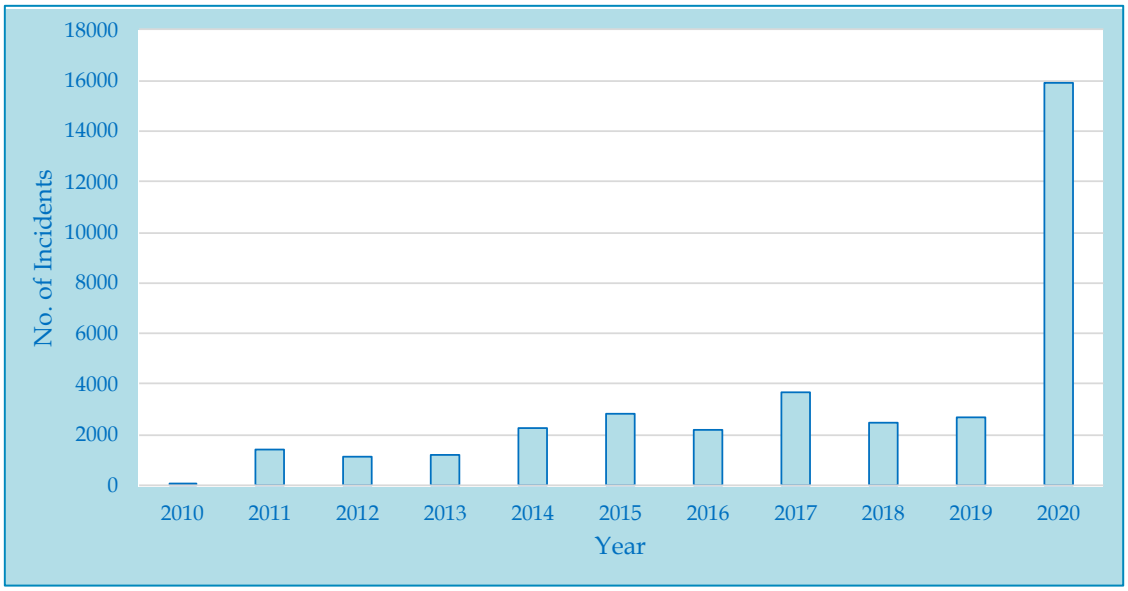
ACTIVITIES & OPERATIONS

INCIDENT HANDLING SUMMARY

Sri Lanka CERT|CC being the national contact point for all cyber security related matters, receives numerous incident reports/complaints relating to the country's national cyber-space from both domestic and international partners.

The types of incidents received by Sri Lanka CERT include incidents related to social networks, email compromise, phishing, web site compromise, scams, malicious software issues and ransomware, privacy violations, financial frauds, compromised unique IP's extracted from the information collected by automated systems operated by international organizations.

Majority of the reported incidents fall in to the category of social media related incidents and on average more than 1000 cases reported each month. Among the social media incidents, as usual Facebook related incidents were the highest. This may be due to increased use of social media, due to COVID-19 pandemic situation.



Graph 1: Total number of social media related incidents

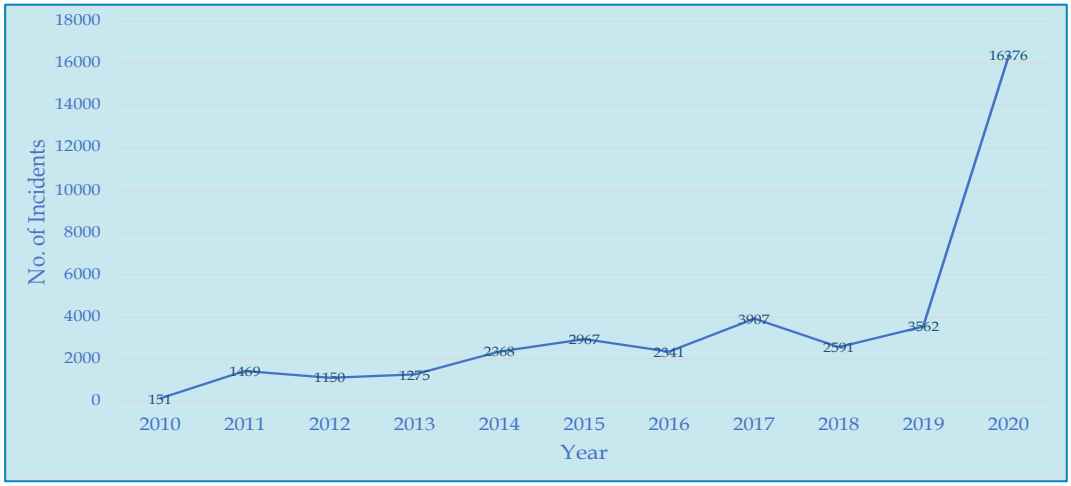
The following table depicts the distribution of various types of incidents reported to Sri Lanka CERT in the years 2019 and 2020. All the incidents reported to Sri Lanka CERT have been resolved satisfactorily.

Incident Type	No of Incidents - 2019	No of Incidents - 2020
DDOS	2	1
Ransomware	6	24
Abuse/Hate/Privacy violation	307	70
Malicious Software issues	8	9
Phone Hacking	1	6
Scams	5	157
Phishing	5	17
Website Compromise	175	85
Financial/Email frauds	7	57
Intellectual property violation	1	1
Server Compromised	2	6
Social media	2662	15895
Other	364	48

Table 1: Number of reported incidents in years 2019 & 2020

Through an analysis of the cyber security related data collected by the Sri Lanka CERT|CC during the years 2019 and 2020 following observations can be made;

i. Number of reported cases related to privacy violations has been decreased during the year 2020.
ii. Financial frauds targeting local importers and exporters have seen a massive upturn during the year 2020 compared to 2019.
iii. There has been a significant increase in the spread of ransomware and malicious software during the year of 2020, where sensitive data belong to both individuals as well as corporate businesses have been made unavailable through encrypting, erasing or modifying data.
iv. A significant number of web site compromises targeting government and private sector organizations were recorded in 2020. However, there is a notable 48% decrease when comparing to year 2019.
v. Incidents reported to Sri Lanka CERT have increased to 16,376 in the year 2020. In the year 2019, 3566 incidents were reported. This is nearly a 460% increase in reported incidents compared to the year 2019.



Graph 2: Total number of reported incidents

CONSULTANCY SERVICES

Sri Lanka CERT continues to provide consultancy services in response to requests made – particularly from government departments. Below are the main consultancy assignments undertaken by CERT during the year;

i. Technical Review Committee (TEC) member of procurement of email solution for a Bank
ii. TEC member of Privileged Access Management (PAM) for a Bank
iii. TEC member of procurement of email solution for a Bank
iv. TEC member of procurement of AV for ATM network of a Bank
v. TEC member of Central Bank of Sri Lanka Procurement of Reserve Management System
vi. Technical Expert of the Presidential Commission on Easter Sunday attack
vii. Curriculum development for Certificate Course in Cyber Security conducted by a National University
viii. Conducted a training program on 'Cyber security incident response' for an Asian Country's Government Cyber Security Bureau.

INFORMATION SECURITY MANAGED SERVICES

i. CERT was able to deliver security managed services with following services;
   - External penetration testing
   - Internal penetration testing
   - Device configuration reviews
   - Network architecture reviews
   - Application security assessments
   - Sever OS configuration reviews

ii. Managed services were provided for on private organization and two government organizations during the year.

APPLICATION SECURITY AUDITS

i. Over 41 Application Security Audits were performed. This includes both Web and Mobile Security Audits.
ii. Daily monitoring of Defaced Websites was done and identified 71 such sites.
iii. Continuous monitoring for potential cyber-attacks related to COVID-19 pandemic and Defaced Websites.
iv. Monitoring of security breaches before the identified special dates of the year.
v. Completed 83 Annual Website Assessments.
vi. Security assessments for 102 Urgent Government Website Audits were completed before November 2020.

TRAINING/ EDUCATION SERVICES

In order to fulfill its mandate to create awareness and build IS skills within the constituency; Sri Lanka CERT continues to organize training programs and education sessions targeting various audiences including CIOs, Engineers, System Administrators, Banking and Telecom Sector Staff, Students, and General Public.

AWARENESS PROGRAMS AND TRAINING SESSIONS

During the year 2020 Sri Lanka CERT conducted the following training and awareness programs successfully:

i. Cyber security awareness session for Internet Society of Sri Lanka.
ii. Session on online safety for ICT teachers.
iii. Session on cyber security fundamentals for government officers.
iv. Participated in the webinar 'Ignite educational Forum 2020' organized for general public.
v. Session on Information security and social media ethics for Postal department.
vi. Webinar on 'Digital forensic procedures and interesting artifacts' for APCERT Community.
vii. Social Media Campaign for the public through the official Sri Lanka CERT|CC Facebook page.
viii. Work from Home Guidelines and awareness webinar for the public and Administrators shared through Official Public channels.
ix. Information Security and Digital Signatures online session for Law student and Government officers.
x. Awareness session for Inland Revenue Department on Introduction to Cyber Threats, Social Media and Mitigation.
xi. Countermeasures and Forensics Webinar for university students participated as a panelist.
xii. Webinar on Cyber security and cyber bullying for public awareness.
xiii. Webinar on Cyber Hygiene & Safety for public awareness.
xiv. Webinar on Introduction to CERT & Cyber safety to University Students.
xv. Cyber Guardian e-Newsletter published every month for School Children.
xvi. Participated as panelists at Women IGF 2020 Webinar.

AWARENESS THROUGH ELECTRONIC/ PRINT MEDIA

Conducted following awareness sessions.

i. Fifteen voice cuts for radio channels
ii. Six video cuts for TV channels
iii. Two Radio programs
iv. Three live TV programs
v. Information for seven newspaper articles
vi. Seven Facebook live sessions

ANNUAL CYBER SECURITY WEEK 2020 (eCSW 2020)

Following activities were completed during the e-Cyber Security Week (eCSW 2020);

i. Conducted Hacking Challenge –28th October 2020
ii. This year's theme was "Pandemic… the new Cyber norm"

iii. More than 900 participants for the online sessions- 19th to 23rd October 2020

iv. Following presentations were delivered during the conference
- Cyber security strategy of Sri Lanka -by Sri Lanka CERT
- Covid-19, SARS and Ebola Vs Defacement, Phishing and DDoS-What's the difference? -by Cyber4Dev, EU
- ATM frauds on the rise -by Sri Lanka CERT
- Understanding malicious activities from distributed honeypots -by APNIC
- Impact of the telecommunications network on national security -by TRC, Sri Lanka
- Cyber security during Covid-19 -by ST Engineering
- How to safeguard from cyber related crimes in Sri Lanka -by Sri Lanka Police
- A way forward to secure your website -by Sri Lanka CERT
- DNS ecosystem security-by ICANN
- Business email compromise cases/money laundry/cyber profiling -by Interpol
- Virtual learning environments and the impact to the learning today and beyond -by University of Queensland
- Security analytics -Detecting threat evading the radar -by CISCO

v. Panel Discussions;
- Challenges faced during COVID-19 lockdown period in Sri Lanka
- Challenges in addressing cybercrime in Sri Lanka

SECURITY ALERTS

i. An Average of 1000 compromised IPs per month were informed to ISPs.

ii. 38 critical security alerts were published and sent to subscribers.

PUBLICATIONS

i. Website

The Sri Lanka CERT website publishes security related awareness bulletins for the public via News Alerts and a Knowledge Base. Glossaries, case studies and FAQs are among some of the other published items.

ii. E-mails

Disseminating security related information via e-mail alerts to Sri Lanka CERT website subscribers.

iii. Newspapers/media

Sri Lanka CERT continues to educate the general public through the electronic and print media about emerging cyber security threats and vulnerabilities with recommendations on how to safeguard against these attacks.

INFRASTRUCTURE DEVELOPMENT & CAPACITY BUILDING OF CERT STAFF

INTERNAL INFRASTRUCTURE & PROCESS IMPROVEMENT

i. Implemented few proposed recommendations of SIM3 Maturity Model assessed by Estonian experts.

ii. Developed the new website for Sri Lanka CERT|CC which is at the final stage.
iii. Performed Server Hardening for Web hosting in the LGC Premises.
iv. Configured the CERT Internal Systems.
v. Developed a Training Book for Interns.
vi. Developed guideline for "best practices for secure website development".
vii. Drafted the communication Specialist SOP with the support of Cyber4Dev.

LOCAL

Staff members of Sri Lanka CERT participated in following capacity building activities;

i. RTIR Configuration workshop (CERT/Cyber4Dev)
ii. Crisis Management (Cyber4Dev)
iii. Workshop on presentations (Cyber4Dev)

INTERNATIONAL

i. DNS Ecosystem Security (Teleconference)
ii. Training on "Safeguarding Critical National Infrastructure (CNI) – Risks and Opportunities" (ITU) (Teleconference)
iii. Webinar on Broken Access Control (Open webinar)
iv. Webinar on SQL injection attacks (Open webinar)
v. Webinar on Network Penetration Test (Open webinar)
vi. New Approach for modern threat detection, investigation and response webinar
vii. Webinar on Advanced Network Exploitations (Open webinar)
viii. OWASP May webinar on Network Penetration testing
ix. Webinar on Digital Forensics - Volatility & Autopsy (Open webinar)
x. Webinar on Hacking Docker Containers (Open webinar)
xi. Webinar on Cyber Incident Planning and Response (ISACA)
xii. Webinar on Learn to Think Like a Hacker to Stop Attacks Faster Strengthen Your Security Posture with the MITRE ATT&CK Framework (ISACA)
xiii. Webinar on Hacking iOS apps for beginners (Open webinar)
xiv. Webinar by ISMG on Cloud Security
xv. Webinar on Why Patch if you don't Fix it? (ISACA)
xvi. Webinar on Introduction to the Risk IT Framework (ISACA)
xvii. Webinar on 'Hacking and Protecting My Wi-Fi by condition zebra (Open webinar)
xviii. Webinar on Android application hacking for beginners (Open webinar)
xix. Webinar on Mac forensics, Drone Forensics, FTK tutorial (by Credence Security)
xx. Teleconference on Combatting Financial Frauds through Effective Money Interception Mechanisms (Interpol)
xxi. Email based Attacks and Mitigation (Teleconference)
xxii. Blue team training (Webinar by Soteria)
xxiii. Cyber Emergency Preparedness & Management Training (by Cyber4Dev)
xxiv. Webinar on Intellectual Property and Patent Rights (FITIS)

xxv. Advanced CSIRT Technical Training (by Cyber4Dev)
xxvi. Web Log Analysis Training (by Cyber4Dev)
xxvii. Webinar on 'Sharpen up Cyber Security Defenses for the New Normal with an Agile, Flexible, and Predictive Strategy' (ISACA)

PROJECTS

SPECIAL PROJECTS

Cyber Security Projects with European Union (Cyber4Dev)

i. Sponsored two CERT staff to participate for APRICOT conference (Australia)
ii. Supported SIM3 implementation work to develop communication stratify, incident classification, RFC for CERT
iii. Following training programs were conducted for CERT staff in February 2020
   - Workshop on ticketing
   - Briefing on UK Incident Management Model & Briefing on Incident Exercising
   - Technical Exercise Run through & PM Planning session
iv. Following training programs were conducted for CERT staff in Nov-Dec 2020
   - Advanced CSIRT Training (3 days)
   - Ticketing System (1/2 day)
   - Log Analysis (2x ½ days)

NATIONAL PROJECTS

Project Name	Project Status
National Cyber Security Operations Center- NCSOC (on-going)	i. Procurement of Physical space for the monitoring center- Procurement - Completed ii. Procurement of hardware for the production data center – On going iii. Procurement of Production data center – In progress iv. Procurement of building material for monitoring center implementation- In progress v. Supply, delivery and installation of raised floor- In Progress
Implementation of National Certification Authority-NCA (in progress	i. Conducted the key generation ceremony in February 2020 ii. Completed the point-in-time audit. iii. Initial registration for Registering NCA Root CA in the Common CA Database (CCADB), Completion of the period-in-time audit – In Progress

Cyber Security Capacity and infrastructure development	i. Completed the procurement of computer hardware and software ii. Completed the procurement of event manger and conducted CSW 2019 iii. Completed the procurement and conducting training
National Survey on Information and Cyber Security (In Progress)	i. Public Officer's Information and Cyber Security Readiness Survey - Conducted the survey for 117 organizations ii. Critical Information Infrastructure Readiness Survey - Completed the CI survey for 59 organizations - Data validation was completed for 51 organizations iii. Supply and Demand of Cyber Security Professionals Survey - In Progress iv. Citizen's awareness of information & cyber security including most vulnerable communities - In Progress
Improving the Information and Cyber Security Readiness of the Government Organizations Maintaining Critical Information Infrastructure (10 organizations)	Project in Progress
Development of a Web Portal to increase citizens' awareness on cyber security (www.onlinesafty.lk)	i. Completed the procurement of the website developer ii. Prototype of the web portal is completed iii. Domain name obtained as (www.onlinesafty.lk) from LK domain registry
Development of National Vocational Qualification (NVQ) Standards for Cyber Security	i. Developed the curriculum and the module outline for NVQ level 5 ii. Project in Progress
Development Online Modules on e-Learning for Government Officers	Project in Progress
Cyber Security Capacity building program	Project in Progress

INTERNATIONAL COLLABORATION

ACTIVITIES WITH APCERT

i. Participated for six APCERT steering committee meetings including at APRICOT 2020 (Australia)
ii. Continuing with network monitoring project "Tsubame" with JPCERT|CC
iii. Organized and conducted meetings with the working group members as the Convener of APCERT working group – Critical Infrastructure Protection
iv. Participated for APCERT working group teleconferences- Policy and Planning, Membership
v. Conducted APCERT online training on "Digital forensic procedures and interesting artifacts" for the APCERT members
vi. Participated for APCERT cyber drill 2020 working group discussions
vii. Participating APCERT cyber drill 2020
viii. Participated for APCERT AGM Program Committee Meeting
ix. Sponsored FIRST and APNIC to obtain the APCERT membership
x. APCERT AGM and Conference 2020 (Teleconference)
    - Member of the program committee of AGM
    - Presented the progress of Critical Infrastructure Protection working group at the AGM
    - Contributed to several APCERT working groups
    - Proposed to have 2021 APCERT AGM to be in Sri Lanka
    - Participated for the APCERT steering committee election 2020-2022

ACTIVITIES WITH CAMP

i. Re-elected as a member of the CAMP Operations Committee for the year 2020-2021
ii. Participated for four CAMP operations committee meetings
iii. CAMP AGM and GCCD Cyber Security Seminar
    - Leading processes and procedures relevant to membership component in CAMP OC
    - Won the Best Operations Committee Member Award during the AGM
    - Made new contacts with cyber security related organization
iv. Reviewed membership application of Nicaragua TELCOR
v. Prepared an article on "Key Generation Ceremony of the National Certification Authority of Sri Lanka" for CAMP Newsletter
vi. Participated in offline discussions on CAMP AGM 2020
vii. Prepared an award acceptance speech video (Best OC member) to present in AGM 2020
viii. Participated for CAMP AGM 2020 and GCCD seminar (online)
ix. Reviewed membership application of Nepal CSRI
x. Participated for CAMP Regional Forum for Arabic Region representing CAMP OC
xi. Reviewed and discussed about R&R arrangements

xii. Reviewed, discussed and finalized the suggestions for implementing Working Groups within CAMP

OTHER ACTIVITIES

i. Delivered a presentation on ITU Session on "National experiences and implications for the future related to COVID-19"

ACHIEVEMENTS

CYBER SECURITY BILL

The Cyber Security Bill was drafted, revised and finalized. Several meetings were held with the stakeholders before finalizing the bill.

INFORMATION SECURITY FRAMEWORK

Under the development of Information security Framework for government organizations following policies were developed by Sri Lanka CERT and is currently in the review process.

i. Handbook of Information Security – An Implementation Guide
ii. Baselines Security Standards (BSS)
iii. Web Application and Hosting Guidelines
iv. Access Control Policy

CERTIFICATION & MEMBERSHIP

Sri Lanka CERT continues to maintain memberships with following professional organizations;

i. (ISC)2 Colombo Sri Lanka Chapter the local representative organization of International Information Systems Security Certification Consortium.
ii. Membership for Threat Intelligence from ShadowServer.
iii. Membership of FIRST
iv. Membership of APCERT
v. Membership of CAMP, Korea
vi. Membership of TF-CSIRT

FUTURE PLANS

FUTURE PROJECTS TO BE IMPLEMENTED

The following projects are to be initiated, and are intended to serve the constituency directly;

i. Establishment of a Sectoral CERT for Education Sector (EduCERT)

PROJECTS IN CONCEPTUAL STAGE

The following projects are in the conceptual design stage,

i. Establishment of Cybersecurity Call center
ii. Outreach and Awareness Activities
iii. Cyber Security Threat landscape in Sri Lanka
iv. Introduce Post Graduate Programs on Information and Cyber Security in collaboration with a State University

SUMMARY

Sri Lanka CERT believes that it is necessary to conduct awareness campaigns to educate citizens on Information security and basic cyber hygiene in order to enable a secure and trustworthy cyber eco system within the country. It was possible to achieve this up to some extent via online awareness sessions. Even with the Covid-19 pandemic situation Sri Lanka CERT managed to conduct the Cyber Security week in electronic media with the theme "Pandemic… the new Cyber norm" with very good participation.

During this year a majority of the incidents reported to Sri Lanka CERT were related to social networking sites especially Facebook. The web site compromises were also a significant issue to the government organizations and therefore CERT as the agency responsible for incident handling, took steps to conduct website vulnerability assessments of the government organizations and directed the responsible parties to make arrangements to secure their websites.

Sri Lanka CERT is in the process of implementing the National Information and Cyber Security Strategy of Sri Lanka with the involvement of relevant stakeholders. To implement some of the proposed activities of the strategy, Sri Lanka CERT|CC has partnered with NI-CO (Northern Ireland Cooperation Overseas) of European Union to participate in a project called Cyber Resilience for Development (Cyber4Dev) which is jointly supported by the Foreign and Commonwealth Office of UK, Dutch Ministry of Foreign Affairs, and Estonian Information System Authority.

The establishment of National Certification Authority, Drafting the Cyber Security Bill, Development of the Information Security Framework for the government organizations, and the deployment of surveys are some of the main activities carried out during the year targeting the implementation of the National Information and Cyber Security Strategy.

Sri Lanka CERT shall continue to participate in regional events such as the Annual APCERT drill, conferences and also welcomes opportunities to collaborate with its sister CERTs in incident coordination and resolution.

In addition to securing Sri Lanka's cyber space, Sri Lanka CERT is committed to support in securing the information environment in the Asia Pacific region and world with the help of all the CERTs and information security organizations through APCERT and FIRST respectively.