Cyber Security Readiness in Sri Lanka and Way Forward with NCSOC

April 27, 2017

Presented by **Rohana Palliyaguru**

SRI LANKA CERT|CC

Agenda

- Evolution of Cyber Security in Sri Lanka
- Myths in Cyber Security
- Critical Areas of concern
- Way forward with NCSOC
- Challenges

Evolution of Cyber Security in Sri Lanka

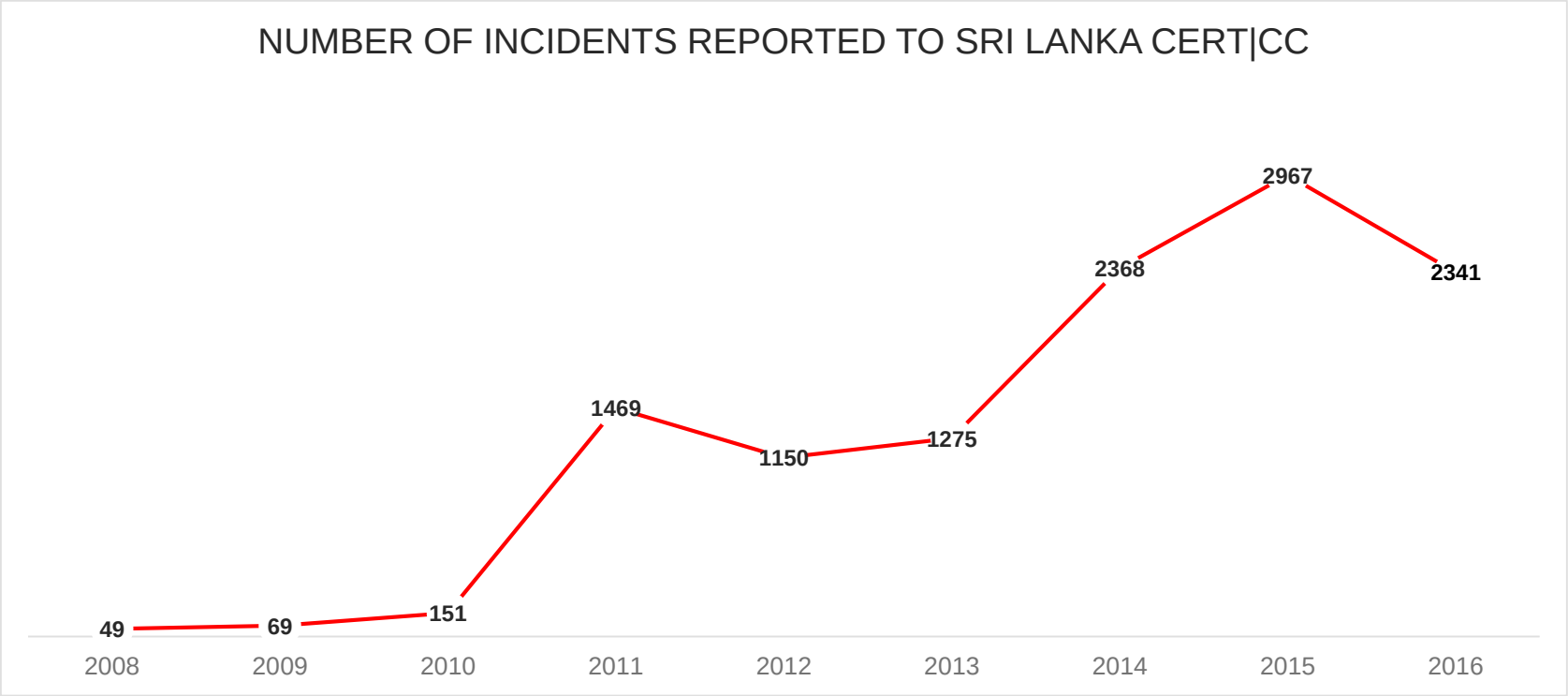
- 2005: ICTA started the e-Sri Lanka initiative
- Sri Lanka was rolling out various electronic on-line services
- E-revenue license, Electronic Travel Authority (ETA), e-Population register etc….
- Web hosting for government organizations
- There was a need to secure those systems

Evolution of Cyber Security in Sri Lanka

- 2006: Establishment of Sri Lanka CERT|CC

- Sri Lanka's National Computer Emergency Readiness Team
- Formed by the ICT Agency of Sri Lanka, as a fully owned subsidiary
- Currently under the Ministry of Telecommunications and Digital Infrastructure
- Non-profit organization
- Primary function is Incident Handling
- Constituency: Public sector, Private sector, General public
- Full member of Asia Pacific CERT and FIRST

Evolution of Cyber Security in Sri Lanka



Evolution of Cyber Security in Sri Lanka

Cyber Crimes Division at CID

- To prosecute cyber security incidents
- Digital forensics lab facility
- Training has been provided by CERT

Evolution of Cyber Security in Sri Lanka

Computer Crimes Act

- **Computer Crimes Act No.24 of 2007**
  - Brought into operation on 15th July 2008
  - Scope of applicability is very broad
  - Covers broad range of offences

Evolution of Cyber Security in Sri Lanka

High Level IS Policy

- Based on ISO 27001
- 17 domains covering most of the areas in IS
- Used by Government Organizations

Myths in Cyber Security

- Firewall will protect our network
- We have done security assessments and hence our systems are secure
- CERT has to secure our systems if they have done security assessments for us
- Security monitoring is not required as our systems are well protected and isolated

Critical Areas of Concern

- Cyber Security Strategy
  - Sri Lanka CERT has already drafted the National Cyber Security Strategy of Sri Lanka
  - Stakeholders consultation should be done
  - Expecting to launch within year 2017

Critical Areas of Concern

International Cooperation

- Sri Lanka Invited to accede Budapest Cybercrime convention(23rd February 2015)
- Acceded to the Cybercrime Convention (29th May 2015)
- 1st Country in South Asia and 2nd Country in Asia after Japan
- Sri Lanka -- ahead of Philippines, South Korea, Malaysia and others
- Fastest ever Accession in Council of Europe history
- Convention in effect -- from 1st September 2015

Critical Areas of Concern

- Continuous Monitoring
  - Security Operations Centers of Internet Service providers
  - Security Operations Centers of Private organizations
  - Lack of National Cyber SOC for government organizations

Way Forward with NCSOC

- Technology

SOCs traditionally were based around a security information and event management (SIEM)

Big Data Security Analytics creates a platform for collecting security data from multiple sources that is far beyond traditional log information

Cyber Security Operations Center

- People

SOC staff includes analysts, security engineers and SOC managers who are seasoned information and communication systems professionals. They are usually trained in computer engineering, cryptography, network engineering, or computer science and are credentialed.

- Process

These processes include business, technology, operational and analytical processes.

Objectives of NCSOC

- Monitor the information systems of the government networks
- Create a pool for resources for protecting the critical infrastructure
- Take proactive measures to secure critical information infrastructure

Specific Problems to be addressed

- To overcome the barrier of identifying the cyber security attacks to the information systems in a proactive manner.
- To overcome the service unavailability due to cyber attacks for government services
- To overcome the problem of selecting various solutions to secure the government services.

Outputs/Outcomes

- Eliminate e-Service interruptions due to cyber attacks
- Increase the use of e-Services securely and with trust
- Provide low cost advanced monitoring services to the government organizations to protect their network systems from cyber attacks
- Availability of national level Cyber Security Operations Center (NCSOC)
- Central body to monitor the network security of Government organizations

Challenges…

- Build trust among the potential stakeholders
- Obtaining continuous support of stakeholders

Phase1-Stakeholders

- Sri Lanka Customs
- Airport and Aviation Services
- Ports Authority
- Department of Immigration and Emigration
- Central Bank
- FinCSIRT

THANK YOU