

The Role of the CERT in Supporting a National Strategy

GLACY International Conference
“Assessing the Threat of Cybercrime”
26-27 March 2015, Colombo, Sri Lanka

By,
Rohana Palliyaguru
Manager-Operations



About Sri Lanka CERT | CC

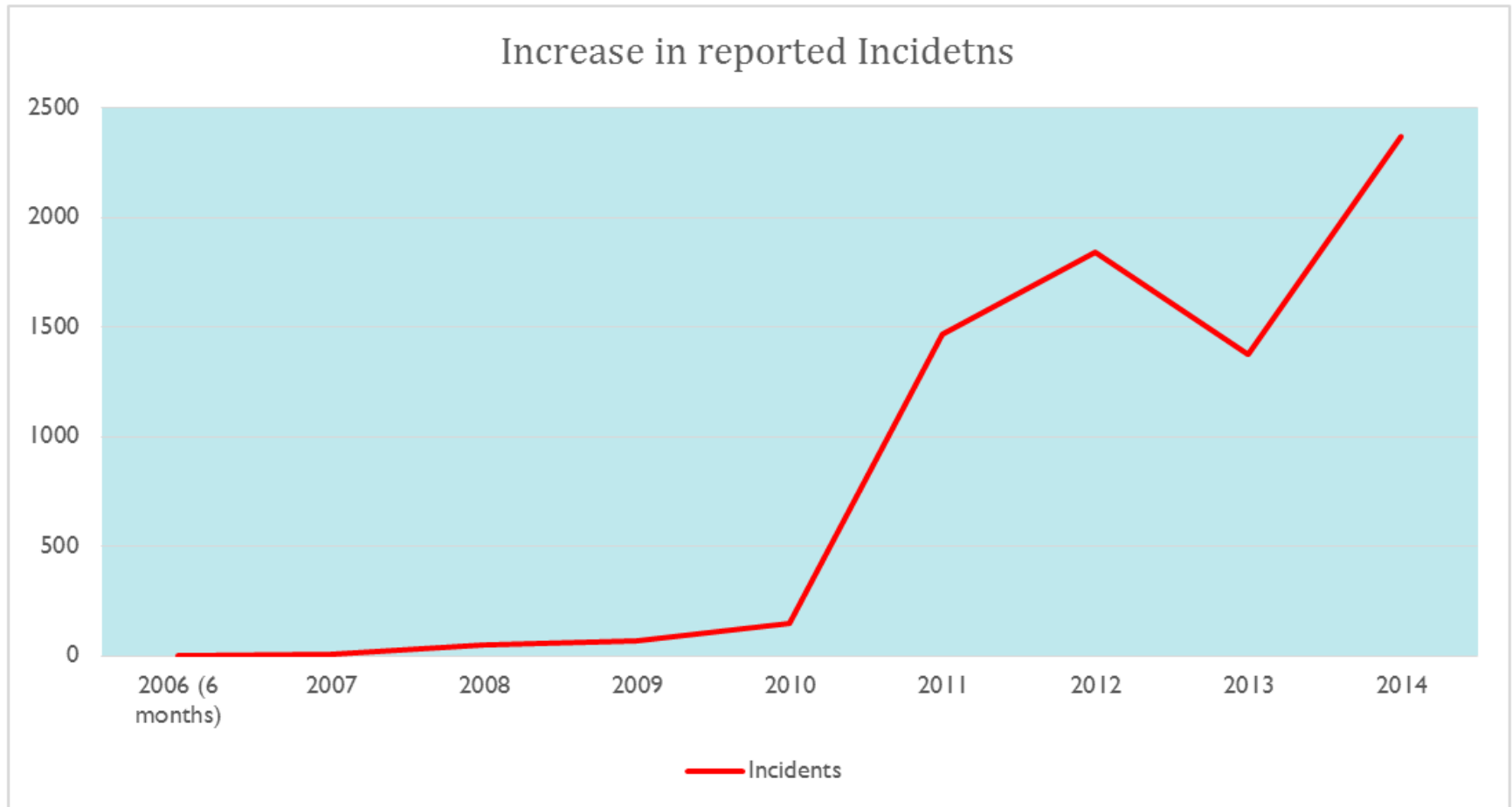
Sri Lanka CERT is the national focal point for cyber security in Sri Lanka.

It is the 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*.

About Sri Lanka CERT | CC

- Established Mid-2006
- Formed by the ICT Agency of Sri Lanka, as a fully owned subsidiary
- Constituency: Public sector, Private sector, General public
- Primary function is Incident Handling, but do involve in awareness, consultancy services, national level IS policy development etc.
- Sri Lanka CERT will assist industry sectors, such as banking, telecommunication and manufacturing to set up their own CSIRTs
- Member of panel of experts in Payment Devices Frauds Act ,No. 20 of 2006.
- Full member of APCERT and FIRST

Cybersecurity Incidents



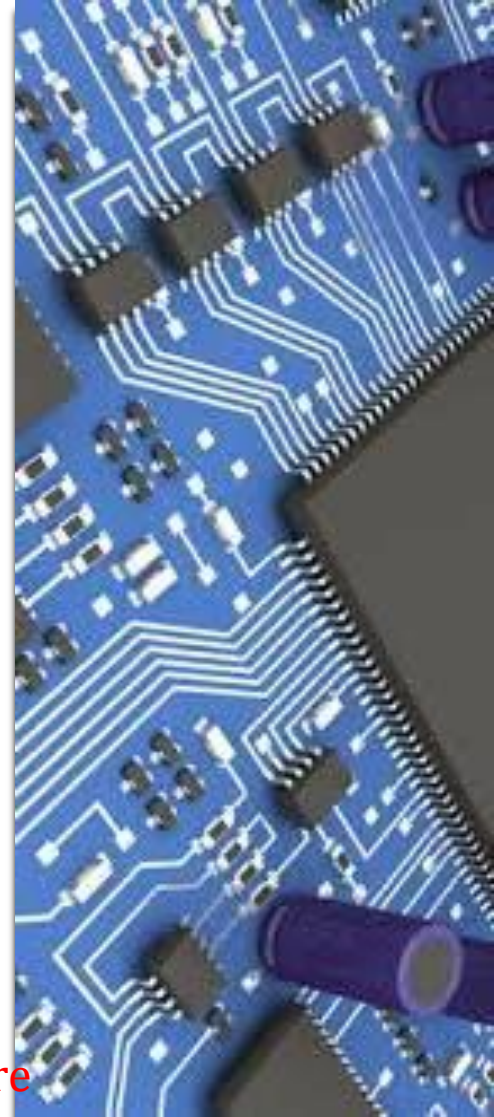
Challenges faced in Cyberspace

- Don't have a Cybersecurity/
Cybercrime Strategy
- Have a Computer Crimes Act. But,
Don't have a Cybercrime Act

Challenges faced in Cyberspace

General Issues

- ICT systems and usage is becoming very complex
- Attention paid for Information Security is insufficient



Challenges faced in Cyberspace

Identification of Cyber Crimes

- Limited reporting of crimes
 - Don't know that they are victims
 - Lack of trust in reporting methods and investigations
 - No guarantee of confidentiality

- Verifying reports/Authenticity of Reports
 - Genuine report or prank?

- Due diligence
 - Reporting of crimes found at workplace.
Professional obligation vs. Personal inconvenience



Challenges faced in Cyberspace

Investigation of Cyber Crimes

- **Gathering of evidence**
 - Lack of training for investigators
 - Maintaining admissibility of evidence
 - Lack of proper structure for cooperation between investigating organizations
 - Poor systems for maintenance of chain of custody
 - Lack of international support

- **Low weight for Digital evidence**
 - Lack of understanding of importance of digital evidence
 - Lack of Legal professionals conversant with CCA



Role of CERT

- Have to help the nation to overcome above challenges
- Contribute to National Cybersecurity Strategy
- Collaborate with law enforcement agencies
- International collaboration

Role of CERT

- Help to protect critical national information infrastructure
- Creating information security awareness
- Run Awareness Programs for the local judiciary to raise awareness of Cybercrimes (attack techniques, potential damage, evidence collection, etc)

THANK YOU



Room 4-112, BMICH,
Buddhaloka Mawatha,
Colombo 07,
Sri Lanka.

Tel: +94 11 269 1692 / 269 5749 / 267 9888
Fax: +94 11 269 1064
E-Mail: cert@cert.gov.lk