



# Proposed Framework For Critical Information Infrastructure Protection (CIIP)

Vijay Mauree  
Manager  
PRD and CERT-MU  
National Computer Board

# Agenda

- What is CIIP?
- International Level
- Mauritius CIIP Framework
  - Critical Sectors
  - Key Players
  - Proposed Recommendations

# What is CIIP?



- Most sectors are dependent on ICT
- 2007 study among parastatals by CERT-MU
  - ❖ 98% of the organisations store information that is critical for them on their computers.
  - ❖ 88% of the organisations will be affected if computers are not available for the day
- Minimise disruptions to critical information infrastructures important to the economy
- Examples of critical information infrastructures:
  - ❖ Utilities, Air/Sea Transport, Telecoms, Finance...
- Is CIIP new ? ...Y2K national coordination ... Business Continuity...

# International Level



- 2002 : UN Resolution 57/239
  - ❖ Member states to address elements to establish a culture of cybersecurity
- 2003: Geneva WSIS Action Line C5
  - ❖ Member states to have a framework to manage information security risks especially for critical sectors
- 2003 : UN Resolution 58/199
  - ❖ Member states to develop strategies for reducing risks to critical information infrastructures

# International Level



## 2007: Generic National framework for CIIP proposed by ITU

- Collection of best practices and good examples
  - Adapted the Swiss CIIP model
  - Proposes a CIIP unit with a 4 pillar approach
    - ❖ Prevention and early warning
    - ❖ Detection
    - ❖ Reaction
    - ❖ Crisis Management
  - Similar to some of the activities of a CERT
- but SCOPE differs ...CIIP pillars are for critical information infrastructures only not for all organisations covered by a national CERT

# International Level



## ➤ Indian Model

- ❖ CERT-In is also leading CIIP activities
- ❖ Optimise resources and limit duplication
- ❖ Legislation underway to give CERT-In investigation powers
- ❖ Currently CERT-In investigates through working arrangements with stakeholders

## ➤ UK Model

- ❖ Centre for Protection of National Infrastructure (CNPI)
- ❖ Operates under the Security Service
- ❖ [www.cnpi.gov.uk](http://www.cnpi.gov.uk)

# National Level



## ➤ NICTSP 2007-2011

- ❖ 2007: Elaboration and endorsement of a National Information Security Strategy (NISS)
- ❖ 2008: CERT-MU set up through MoU with CERT-In (India)
- ❖ 2009: CERT-MU to elaborate the CIIP framework for Mauritius **along Indian model** as per NICTSP and NISS recommendations

## ➤ Possible Mauritian CIIP model

- ❖ Establish sectoral CERTs for Critical sectors
- ❖ CERT-MU to assist sectoral CERTs and liaise with international CERTs where appropriate (including promotion of best practices)
- ❖ High level committee to monitor status and handle crisis

# Mauritius CIIP Framework



- Minimise the nation wide impact of information security disruptions through
  - ❖ Clear leadership for information security risk management national level and at the level of organisations
  - ❖ Development of capabilities for responding to information security incidents impacting critical infrastructures
  - ❖ Promoting the adoption of industry best practices and standards for the protection of information infrastructures

# Critical Sectors



- Based on Y2K experience and augmented by a circular letter to all Ministries by MICT in January 2009
  - Customs
  - Energy
  - Financial Services inc. Banking
  - Government Services
  - Health
  - ICT & Broadcasting
  - Manufacturing
  - Sugar
  - Transport & Logistics
  - Tourism
  - Water Supply

# Proposed Recommendations



- Information security risk management **leadership** at national and organisational level
- **Policy framework** for information security risk management for operators of Critical Infrastructures
- Adoption of information security **best practices and standards**

# Key players in CIIP



- Government
  - ❖ Define goal, policy and roles
- Sector Regulators / Ministries
  - ❖ Enforce Business Continuity of what's critical
- Critical Infrastructure Operators
  - ❖ Assess & Prioritise risks
  - ❖ Identify controls + acceptable risk level
  - ❖ Implement controls
  - ❖ Measure effectiveness

# Leadership



## National Level

- Monitor status of controls in place for all critical infrastructure
- Co-ordination in event of national crisis
- International Co-operation
- Mechanisms for information sharing
- Stakeholders
  - CIIP Co-ordinator (a High level committee)
  - Sector Specific Agencies (e.g. Regulatory Body for each sector)
  - Law Enforcement (Police)
  - CERT-MU
  - Critical information infrastructure Operators
  - Major ICT Vendors

# Leadership



## Organisation level

- ❖ Clear ownership of Information Security and Accountability for the information risks within an organisation at board/top management level
- ❖ Information Security Policy + Review at regular intervals
- ❖ Information Security Risk Management Strategy adopted at board/top management level

# Proposed Recommendations



- Information security risk management **leadership** at national and organisational level
- **Policy framework** for information security risk management for operators of Critical Infrastructures
- Adoption of information security **best practices and standards**

# Policy Framework



## **Based on Indian Model as per recommendations of NISS/NICTSP 2007-2011**

1. Point of contact responsible for coordinating security policy compliance efforts
2. Mandatory information security programme in place
3. Carry out periodic IT Security risk assessment
4. Periodically test and evaluate the adequacy /effectiveness of technical security control measures
  - a. Penetration testing
  - b. Vulnerability Assessment
  - c. Application and Web Security Testing
5. Mandatory annual third party IT Security Audit
6. Mandatory reporting of major information security incidents to CERT-MU

# Policy Framework



## Legal Framework Implications for critical sectors

- Reporting of information security incidents by Critical Information Infrastructure Operators to CERT-MU
- Investigating information security incidents
- Organisations in critical sectors should also develop and implement processes which allow them to recover from information security incidents

# Proposed Recommendations



- Information security risk management **leadership** at national and organisational level
- **Policy framework** for information security risk management for operators of Critical Infrastructures
- Adoption of information security **best practices and standards**

# Information Security Best Practices

**CERT-MU to facilitate the implementation of a 10 Step best practice approach (of Indian Model) at each critical information infrastructure operator .**

(pages 10-11 of draft CIIP framework document)

## **Existing CERT-MU services in that respect**

- Workshops
- Working sessions upon request
- Website
- Email based security alerts upon subscription
- Training sessions (ISO 27001, BS 25999 etc.)



THANK YOU