

## **Proceedings of the Critical Information Infrastructure Protection (CIIP) Workshop held at La Canelle, Domaine Les Pailles and organized by CERT-MU**

### **1. Objective**

The objective of the workshop was to discuss and agree on what would be the important ingredients of a framework for critical information infrastructure at national level. The main outcome of the workshop would be a roadmap for the implementation of critical information infrastructure protection in Mauritius. The target audience was operators of critical information infrastructure in Mauritius.

The Hon. Asraf Dulull, Minister of Information and Communications Technology officially opened the workshop and announced that his ministry was actually working on the setting up of an agency which will be focusing streamlining roles and responsibilities for the resolution of cyber crimes. Mr Suraj Ramgolam, Chairman of the National Computer Board (NCB) mentioned in his speech that protecting critical information infrastructures is essential to ensure the business continuity at national level and to promote Mauritius as a safe destination for business. He also gave an example of how organizations were impacted during the 9/11 terrorist attack on the World Trade Centre in New York in 2001. Mr Dan Faugoo, Executive Director of the NCB emphasized on the role CERT-MU will have to play in the implementation of protection of critical information infrastructures.

### **2. Session 1: Information Security Risk Management Leadership at National Level**

Chairperson: Dr. K Oolun, ICT Authority

Panel Members:

Mr. V. Mauree, Manager – PRD and CERT-MU, NCB

Mr. Prakash Seewoosunkur, IT Executive, Financial Services Commission

Mr. Arvind Kumar Dowlut, Senior Analyst Programmer, Bank of Mauritius

#### **i. Importance of Critical Information Infrastructure Protection at National Level**

*By Mr. Pete Freilinghaus, CEO, Continuity Mauritius*

The first presentation of the workshop has highlighted a very clear need for protection of critical information within the critical sectors and some of the solutions have been talked about. A case study of London Stock exchange is cited to show how the malfunction of the '*TradElec System*' could manage to bring down the whole exchange to halt for 7 hours on the busiest day and its impact on the business. This scenario thus calls for a need for critical information protection.

**ii. Recommendations for Policy Framework for Critical Information Infrastructure Protection**

*By Mr. Vijay Mauree, Manager – PRD and CERT-MU, National Computer Board*

The objective of this presentation was to present the proposed recommendation for the policy framework for the critical information infrastructure protection at national level. It is essential that Mauritius should develop a plan for and develop policies that will enable them to provide reasonable assurance of resiliency and security to support the critical sectors. The critical sectors of Mauritius are listed as follows (*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 (all Ministries, Departments, Municipalities and Parastatals)
- Health
- ICT & Broadcasting
- Manufacturing
- Sugar
- Transport & Logistics
- Tourism
- Water Supply

The recommendations for the policy framework can be summarised as follows:-

- a) Need for leadership in information security risk management at national level and at level of organizations;
- b) Policy framework for information security risk management for critical sector operators;
- c) Adoption of information security best practices.

**iii. Role of CERT-MU**

*By Mr. Kaleem A Usmani, Information Security Consultant-CERT-MU*

In this presentation the role of CERT-MU with respect to CIIP was highlighted.

**iv. Summary of Discussions**

The discussions can be summarized as follows:-

- There is a need on leadership at the national level for Information Security Risk Management  
*It has been agreed that there will be high level committee which will be setup to lead and monitor the status of CIIP at the national level. This committee will have the members from the regulatory authority for each critical sector who will be*

*responsible for monitoring the status of CIIP and Business Continuity for their sector.*

- Guidelines for Information Security Management to be drafted  
*The guidelines for information security management have been stated by operators as a key requirement for being able to implement the policy. There was a general consensus that CERT-MU would have a key role to play in this respect.*
- Establish a forum for Information Sharing among operators within a sector and across sectors.  
*It has been proposed the high level committee that will be set up will need to work out mechanisms for information sharing about incidents and lessons learned among operators within a sector and across sectors in order to ensure that confidential information is not disclosed.*
- It was observed that the list of organisation for government services mentioned in the draft document includes all ministries and departments as well as parastatal organizations and is not limited to only the names of the organizations mentioned in the document. The document will be reflected to amend this.
- Creation of CERTs within each critical sector  
*It is proposed that similar sectoral CERT should be created to handle incidents within each sector and these CERTs will be the main security liaison with CERT-MU on the matters of incident response.*
- Information Security is a business issue, not technology  
*It was noted that Information Security is a management issue rather than technical and management should play a proactive role to establish leadership in establishing proper information security risk management strategies and policies in their organizations to indicate their commitment and also as a matter of good corporate governance.*
- IT Security Audits  
  
*It was noted by operators that the cost of IT Security Audits are quite expensive and that there is a scarcity of qualified firms who can do such audits and most of the time organizations have to resort to overseas. It was highlighted that the criteria for the IT Security Audit would be determined by CERT-MU if we adopt the Indian model and CERT-MU would then have a team of panel auditors which would be hired through an RFP and they would do the audit at a certain cost. It was also noted that the frequency of the audit is not necessarily an issue and it could be either one year or two years. It was highlighted that the IT Security audit would be mandatory for all operators of CII and therefore this would be a legal compliance requirement. It was suggested that the framework be quite flexible and allow for certain period of time to enable organizations to implement the necessary policies and structure before being mandatory.*

- CERT-MU to provide assistance to organizations for Information Security  
*It was proposed that CERT-MU provide technical assistance to organizations for implementation of information security policies and on awareness of information security risk management.*
- The representative of the Police IT Unit made suggested that there is a need to review the requirement of the need for a Judge order for police before investigation can be initiated for such cyber crime incidents. It was noted that this requirement was currently under review for the amendments to the ICT Act being prepared by the State Law Office.

**3. Session 2: Policy Framework for Information Security Risk Management for Operators of Critical Information Infrastructure and Government organisations and mandatory reporting of information security incidents**

Chairperson: Mr. Kapil Reesaul, Senior Executive, Mauritius Telecom

Panel Members:

Mr. Rai Basgeet, Senior Executive-Networks Planning, Mauritius Telecom Ltd

Mr. V. Mulloo, Manager GOC, NCB

Mr. Arvind Kumar Dowlut, Senior Analyst Programmer, Bank of Mauritius

Mr. Sanjeev Jhurry, Information Risk Analyst, Mauritius Banker's Association,

**i. A Case Example - Security Management at Mauritius Telecom,**

*By Mr. Rai Basgeet, Senior Executive-Networks Planning, Mauritius Telecom (MT)*

In the presentation the Mauritius Telecom has presented the security measures they take at their end and also they have talked about the information security management system which MT will be implementing based on ISO/IEC 27001.

**ii. IT Security measures at the Government Online Centre**

*By Mr. Vyankoj Mulloo, GOC, National Computer Board*

Mr Vyankoj Mulloo talked about the security measures adopted at the Government Online Centre (*including physical, network and application security*), which is offering 53 services to the public. The GOC data center hosts all the confidential data of ministries and departments as well as their e-mail service and is currently implementing the ISO 27001 Information Security Standard.

### **iii. Policy Framework proposed based on the Indian Model**

In order to reduce the risk of cyber attacks and improve upon the security posture of critical information infrastructure, Government and critical sector organisations are required to do the following on priority:

- Identify a member of senior management, as Chief Information Security Officer (CISO), knowledgeable in the nature of information security & related issues and designate him/her as a “Point of contact”, responsible for coordinating security policy compliance efforts and to regularly interact with the Computer Emergency Response Team (CERT-MU), which is the nodal agency for coordinating all actions pertaining to cyber security.
- Prepare information security plan and implement the security control measures as per ISO/IEC 27001 and other guidelines/standards, as appropriate.
- Carry out periodic IT security risk assessment and determine acceptable level of risks, consistent with criticality of business/functional requirements, likely impact on business/functions and achievement of organisational goals/objectives.
- Periodically test and evaluate the adequacy and effectiveness of technical security control measures implemented for IT systems and networks. Especially, test and evaluation may become necessary after each significant change to the IT applications/systems/networks and can include, as appropriate the following:
  - Penetration testing (both announced as well as unannounced)
  - Vulnerability Assessment
  - Application Security Testing
  - Web Security Testing
- Carry out audit of Information Infrastructure on an annual basis and when there is major upgrade/change in the IT infrastructure, by an independent IT Security Auditing Organisation
- Report to CERT-MU the cyber security incidents, as and when they occur and the status of the cyber security, periodically.

### **iv. Summary of Discussions**

- Indian Model for Information Security Risk Management  
*It was agreed that the Indian model of information security risk management could be adopted.*
- Human factor to be underestimated in the implementation of Information Security Risk Management

- Reporting of incidents

*It is mentioned that reporting of incidents is a sensitive issue and may be tackled at the level of the different sectors as per the nature of incident of each sector. It has also been pointed out that, currently incidents are reported to the regulators (such as MT, EMTEL etc) and it is recommended that the incidents should be reported to CERT-MU by regulators and an MOU to be worked out between the regulators and CERT-MU for reporting incidents. Furthermore it is recommended to establish a Disclosure Policy and Protocol within and across critical sectors.*

- Reporting of incident to CERT-MU is essential for establishing threat profile to identify the main categories of incidents for each sector and also the origin of the attacks in order to clearly identify instruments for international co-operation. In order to maintain national threat profile, it is recommended that incidents should be reported to the regulatory authority which will then report it to CERT-MU promptly. Again there will be a need to include this requirement in the legal framework.
- Legislation required to implement the recommendations  
*It was noted that there is a need to have a legislation to implement the above mentioned recommendations.*

#### **4. Session 3: Adoption of Information Security Best Practices and Standards**

Chairperson: Mr. Dan Faugoo, Executive Director, NCB

Panel Members:

Dr K. Oolun, Executive Director, ICT Authority

Mr. V. Moonegan, President, OTAM

Mr. S. Bissessur, Project Manager, IT Security Unit, Ministry of ICT

Mr. K. Usmani, Information Security Consultant, CERT-MU

Mr. Rai Basgeet, Senior Executive-Networks Planning, Mauritius Telecom Ltd

Mr. Kapil Reesaul, Senior Executive, Mauritius Telecom Ltd

It was proposed in the draft document on the policy framework for CIIP that the following 10 step approach be adopted as a best practice at national level by Critical Information Infrastructure operators.

- 1) Identification of a Point-of-Contact at the level of each organisation for coordinating security policy implementation efforts and communication with CERT-MU.
- 2) Develop and implement Information Security Awareness Programme for the organisation,

- 3) Determination of general risk environment of the organization (low/medium/ high) depending on the nature of web & networking environment, criticality of business functions and impact of security incidents on the organization, business activities, assets/resources and individuals.
- 4) Status appraisal and gap analysis against international security best practices-ISO-27001.
- 5) Risk assessment covering evaluation of threat perception and technical & operational vulnerabilities.
- 6) Comprehensive risk mitigation plan including selection of appropriate security controls as per international security best practices and standards such as ISO-27001.
- 7) Documentation of agreed security control measures in the form of security policy manual, procedure manual and work instructions.
- 8) Implementation of security control measures (Managerial, Technical & operational).
- 9) Testing & evaluation of technical security control measures for their adequacy & effectiveness and audit of IT applications/systems/ networks by an independent IT security auditing organization (Penetration testing, vulnerability assessment, application security testing, web security testing, LAN audits etc.).
- 10) Information Security Management assessment and certification against ISO 27001 standard, preferably by an independent & accredited organization.

#### **i. Summary of Discussions**

On the basis of the above proposal, it was agreed during the brainstorming session that the above mentioned practices should be adapted at the national and the following were recommended.

- *CERT-MU will promote the adoption of Information security best practices at the national level in accordance with requirement of the organization(s).*
- *It is essential for the organizations operating critical information infrastructure to adopt industry best practices or ISO 27001.*

## 5. Next Step

It was agreed that the proceedings for the workshop would be put on the CERT-MU website and participants would have till 16<sup>th</sup> September 2009 (*i.e. the deadline*) to submit their feedback or other additional suggestions as may be required. A workgroup composed of the panel members of the workshop has been setup to review and update the draft framework for CIIP. The updated document would be submitted to the Ministry of ICT thereafter for approval.

CERT-MU Website Address: [www.cert-mu.org.mu](http://www.cert-mu.org.mu)

Send your suggestions on: [info@cert-mu.gov.mu](mailto:info@cert-mu.gov.mu)