

Summary of CIIP Workshop

Session 1 - Information Security Risk Management Leadership at National Level

- Establish a forum for Information Sharing
- Guidelines for Information Security Management to be drafted
- There is a need on leadership at the national level for Information Security Risk Management
- Creation of CERTs within each critical sector
- Organization to adopt Information Security Risk Management
- CERT-MU to provide assistance to organizations for Information Security
- Information Security is a business issue, not technology
- Judge order in chamber for police to be reviewed for CIIP
- Legal aspect of security is important, but legislation should consider the practical aspects of enforcement so as not to overburden organizations.

Session 2 - Framework for Information Security Risk Management for Operators of Critical Information Infrastructure and Government organisations and mandatory reporting of information security incidents

- Indian Model for Information Security Risk Management
- Human factor to be underestimated in the implementation of Information Security Risk Management
- Reporting of incidents
 - ❑ Sensitive Issue
 - ❑ Different cultures of reporting among different sectors
 - ❑ Currently incidents are reported to the Regulator
 - ❑ Maintain same + regulator to report incident to CERT-MU
 - ❑ MOU to be worked out between regulators and CERT-MU
 - ❑ Disclosure Policy and Protocol to be established
 - Within and Across Sector
- Reporting of incident to CERT-MU is essential for establishing threat profile
- Legislation required to implement the recommendations

Session 3: -Adoption of Information Security Best Practices and Standards

- **CERT-MU to promote the adoption of Information Security Best Practices**
- **Organisations operating CII need to adopt industry best practices or ISO 27001**

Proceedings of Workshop would be available on CERT-MU website: <http://www.cert-mu.org.mu>

Kindly send comments on info@cert-mu.gov.mu by 16th September 2009.