Chapter 5

Findings and Recommendations

Based on the guidelines, data and analysis mentioned in the preceding chapters findings and recommendation are as follow :

Findings:-

1. India has taken up the steps (membership and follow up) towards Common Criteria Recognition Agreement (CCRA). In CCRA, about 26 countries are members. Out of these 17 countries are authorizing nations and 9 countries are consuming nations. If, the equipment is evaluated and security certified in authorizing nation'saccredited lab then it will be accepted in all other member country. However, during the study it has been observed that only one lab have been accredited in India for the evaluation and certification of IT product so far. Also, the industries have not been made mandatory to use only security certified product.
2. Government of India has set up computer emergency response team (CERT-IN). It has been observed that in 2010, 2011, 2012, 2013 and 2014, total 10315 , 13301, 22060, 71780 and 130338 incidents of cyber were reported.From

While analyzing these data it has been observed that incidents of cyber attacks are increasing. Therefore, serious and focus approach is required to protect the critical infrastructure.

3. Government of India has made enacted the IT Act in 2000. Subsequently, it was observed that the said act is not sufficient to deal the cyber security issues. Accordingly, the said act was amended in 2008. By such provisions, the Government authorities are well equipped to handle and protect the system.

4. In 2013, Government of India has issued the cyber security policy.The Cyber Security Policy aims at protection of information infrastructure in cyberspace, reduce vulnerabilities, build capabilities to prevent and respond to cyber threats and minimize damage from cyber incidents through a combination of institutional structures, people, process, technology and cooperation. The objective of this policy in broad terms is to create a secure cyberspace ecosystem and strengthen the regulatory framework.

Creating a workforce of 500,000 professionals needs further deliberations as to whether this workforce will be trained to simply monitor the cyberspace or trained to acquire offensive as well as defensive cyber security skill sets. Indigenous development of cyber security solutions as enumerated in the policy is laudable but these solutions may not completely tide over the supply chain risks and would also require building testing infrastructure and facilities of global standards for evaluation.

The key to success of National Cyber Security policy lies in its effective implementation. The much talked about public-private partnership in this policy, if implemented in true spirit, will go a long way in creating solutions to the ever-changing threat landscape.

5. For protection of Telecommunication infrastructure, Government of India has issued the license amendment on 31st May 2011. Various concern of the security related matters have been addressed in the license amendment. As per amendment,w.e.f. 1.4.2013, the Telecom Service Providers will induct only those network elements, which have been got certified from labs in India. The effective date for certification of network elements has been extended many times, but the security testing of Telecom network elements have not been commenced so far. While discussing, with the officers responsible it was revealed that the commencement of testing may still take further time due to non availability of regular and suitable structure for the said work. The proposal for establishment of Telecom Security Directorate, which consist the requirement of Telecom Testing and Security Certification, Centralized Monitoring System, Security Audit etc has been moved by the security wing of DOT, but the same has not been approved so far.
6. Some cyber-attacks which are possible as given in chapter 2. Out of these following attacks needs special mention which are very frequently reported in CERT-IN.

- Phishing
- Network / Scanning/Probing

- Virus /Malicious Code
- Website Defacements
- Spam
- Website Intrusion & Malware Propagation
- Others

7. As per National Cyber security policy, a sectoral CERT was to be opened, but no action has been taken so far.
8. Regarding challenges, it was also revealed that many people are not adequately aware about the cyber security precautions like use USB, secure E-mail, use of authentic antivirus, strong password, updation of operating system etc. Also there is shortage of security experts in the field of Telecommunication, IT , police etc.

Recommendations

1. Based the study it is concluded that cyber security is a very important issue at present. Digital India is flagship programme of present Government. Therefore along with the provision of broadband upto village level, security of network and application is also important.
2. The general public using the internet, smart phones, laptop computers, social media is to be made aware about the cyber security threats and precautions. For general awareness of cyber security among people and employees workshop/ trainings may be organized.