Strategic Approach

Consistent with the need, the primary objectives for securing country's cyber space are:

- Preventing cyber attacks against the country's critical infrastructures
- Reduce national vulnerability to cyber attacks
- Minimise damage and recovery time from cyber attacks

Actions to secure cyberspace include:

- Forensics and attack attribution
- Protection of networks and systems critical to national security
- Early watch and warnings
- Protection against organized attacks capable of inflicting debilitating damage to the economy
- research and technology development that will enable the critical infrastructure organisations to secure their IT assets

To pursue the strategic objectives the following major initiatives have been identified:

- Security Policy, Compliance and Assurance
- Security Incident - Early Warning & Response
- Security training - skills/competence development & user end awareness.
- Security R&D for Securing the Infrastructure, meeting the domain specific needs and enabling technologies
- Security - Promotion & Publicity

I. Security Policy, Compliance and Assurance

Focus: Creation, Establishment and operation of Cyber Security Assurance Framework aimed at enabling Government, Critical Infrastructure Organisations and other key IT users of nation's economy

(a) Critical Inforamtion Infrastructure Protection

Many of the critical services that are essential to the well being of the economy are increasingly becoming dependent on IT. As such, the Government is making efforts to identify the core services that need to be protected from electronic attacks and is seeking to work with organisations responsible for these systems so that their services are secured in a way that is proportional to the threat perception. The primary focus of these efforts is to secure the information resources belonging to Government as well as those in the critical sectors. The critical sectors include Defence, Finance, Energy, Transportation and Telecommunications. Consequently, many in the industry and critical infrastructure organizations have come to recognize that their continued ability to gain consumer confidence will depend on improved software development, systems engineering practices and the adoption of strengthened security models and best practices.

(b) Cyber Security Assurance Framework

Cyber Security Assurance Framework is a National framework for "Cyber Security Assurance" to assist National level efforts in protecting critical information infrastructure. It aims to cater to the security assurance needs of Government and critical infrastructure organisations through "Enabling and Endorsing" actions.

Enabling actions are essentially Promotional/Advisory/Regulatory in nature and are best done by Govt. or its authorized entity that can be seen and perceived as independent of bias and/or commercial interests. They involve publication of "National Security Policy Compliance requirements" and IT security guidelines and supporting documents to facilitate IT security implementation and compliance

Endorsing actions are essentially commercial in nature and may involve more than one service provider offering commercial services after having fulfilled requisite qualification criteria and demonstrated ability prior to empanelment. These include

- Assessment and certification of compliance to IT security best practices, standards and guidelines (Ex. ISO 27001/BS 7799 ISMS certification, IS system audits etc)
- IT Security product evaluation and certification as per 'Common Criteria' standard ISO 15408 and Crypto module verification standards
- IT security manpower training and other services to assist user in IT security implementation and compliance

Trusted company certification

With India emerging as a leading outsourcing partner, there is a need to address perceptible gap among Indian IT/ITES/BPOs in respect of compliance to international standards and best practices on security and privacy. Today, although increasing number of organisations in India have aligned their internal processes and practices to international standards such as ISO 9000, CMM, Six Sigma, Total Quality Management, ISO 27001

etc., it is to be noted that existing models such as SEI CMM levels cover exclusively software development processes and do not address security issues. As such, there is a need for a comprehensive assurance framework that can enable compliance within the country and provide assurance on compliance to out sourcing organizations and rest of the world. Accordingly, efforts are on to create a model that is based on self-certification concept and on the lines of Software capability maturity model (SW-CMM) of CMU, USA.

II. Security incident - Early Warning & Response

Focus: Creation of National Cyber Alert System for Rapid identification & response to security incidents and information exchange to reduce the risk of cyber threat and resultant effects.

(a) Rapid identification, information exchange, and remediation can often mitigate the damage caused by malicious cyberspace activity. For those activities to take place effectively at a national level, it requires a partnership between government and industry to perform analyses, issue warnings, and coordinate response efforts. Because no cyber security plan can be impervious to concerted and intelligent attacks, information systems must be able to operate while under attack and also have the resilience to restore full operations in their wake. The National Cyber Alert System will involve critical infrastructure organizations, public and private institutions to perform analysis, conduct watch and warning activities, enable information exchange, and facilitate restoration efforts.

(b) The essential actions under National Cyber Alert System include:

- Identification of focal points in the critical infrastructure
- Establish a public-private architecture for responding to national - level cyber incidents
- Tactical and strategic analysis of cyber attacks and vulnerability assessments;
- Expand the Cyber Warning and Information Network to support the role of Government in coordinating crisis management for cyberspace security;
- Improve national incident response capabilities (CERT-In and Sectoral CERTs)
- Exercise cyber security continuity plans and drills

(c) Creation and Augmentation of Response Capabilities

Augmentation of CERT-In: CERT-In is operational since January 2004 and is catering to the security needs of Indian Cyber community, especially the Critical Information Infrastructure. In line with the expectation of the user community and various stake holders, there is a need to augment the facilities at CERT-In in terms of Manpower, Communication systems, tools, etc. for vulnerability prediction, analysis & mitigation, Cyber forensics/artifact analysis, Cyber space monitoring & interception Capabilities and Critical information infrastructure Security health check. The National Information Board and National Security Council have endorsed the need for augmentation of facilities at CERT-In.

Creation/augmentation of Sectoral CERTs: For an effective National Cyber Security Alert System, there is a need to create sectoral CERTs to cater to the very specific domain needs of different sectors. In this direction sectoral CERTs have been established by Army, Air force and Navy in Defense sector, IDRBT in Finance sector. But the facilities of these sectoral CERTs are at primitive levels and need to be augmented to meet the needs of respective sectors. Similarity sectoral CERTs with state-of-the-art facilities need to be created in other critical sectors such as Aviation, Energy, Telecommunication, Railways etc.

(d) International cooperation and information sharing

The cyber threat sources and attacks span across countries. As such as there is a need to enhanced global cooperation among security agencies, CERTs and Law Enforcement agencies of various countries to effectively mitigate cyber threats. Accordingly it vital to have well developed Cyber Security and Information Assurance research and development Programme which is executed through different government agencies in broad collaboration with private sectors, partners and stakeholders in academia, national and international agencies.

In this context the priorities for collaboration are:

- Cyber Security and Information Assurance Technology to prevent, protect against, detecting, responding, and recovering from cyber attacks in critical information infrastructure that may have large-scale consequences.
- Collaboration for training personnel in implementing and monitoring secure government intranets and cyber space
- Joint R&D projects in the area of Steganography, water marking of documents, security of next generation networks and Cyber Forensics
- Coordination in early warning, threat & vulnerability analysis and incident tracking
- Cyber security drills/exercises to test the vulnerability & preparedness of critical sectors

III. Security training - Security, Digital Evidence & Forensics

Focus - To meet the specific needs of Law Enforcement, Judiciary and other users such as E-Governance project owners catering for

- *A baseline for IT Security awareness*
- *Skill & Competence development*
- *Advanced Manpower Certification programmes*

Many cyber vulnerabilities exist because of lack of cyber security awareness on the part of computer users, system/network administrators, technology developers, auditors, Chief Information Officers (CIOs), Chief Executive Officers (CEOs), and Corporates. A lack of trained personnel and the absence of widely accepted, multi-level certification programs for cyber security professionals complicate the task of addressing cyber vulnerabilities. This Cyber Security Strategy identifies following major actions and initiatives for user awareness, education, and training:

- Promote a comprehensive national awareness program
- Foster adequate training and education programs to support the Nation's cyber security needs
- Increase the efficiency of existing cyber security training programs and devise domain specific training programs (ex: Law Enforcement, Judiciary, E-Governance etc)
- Promote private-sector support for well-coordinated, widely recognized professional cyber security certifications.

IV. Security R&D

Focus: Facilitating Basic research, Technology demonstration and Proof-of concept and R&D test bed projects

(a) Indigenous R&D is an essential component of national information security measure due to various reasons- a major one being export restrictions on sophisticated products by advanced countries. Second major reason for undertaking R&D is to build confidence that an imported IT security product itself does not turn out to be a veiled security threat. Other benefits include creation of knowledge and expertise to face new and emerging

security challenges, to produce cost-effective, tailor-made indigenous security solutions and even compete for export market in information security products and services. Success in technological innovation is significantly facilitated by a sound S&T environment. Resources like skilled manpower and infrastructure created through pre-competitive public funded projects provide much needed inputs to entrepreneurs to be globally competitive through further R&D. Private sector is expected to play a key role in meeting needs of short term R&D leading to commercially viable products. Besides in-house R&D, this sector may find it attractive to undertake collaborative R&D with leading research organisations.

Top

Content owned & provided by Department Of Electronics & Information Technology, Government Of India
Page last updated on February 10, 2015 Site Counter: 1,723,498