GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:3456
ANSWERED ON:18.03.2015
SECURITY AUDIT OF COMPUTERS
Boianapalli Shri Vinod Kumar;Raajhaa Shri Anwhar

Will the Minister of COMMUNICATIONS AND INFORMATION TECHNOLOGY be pleased to state:

-

(a) whether the Government proposes to conduct a full security audit of all official computers and security vetting of staff of major Ministries and departments in the wake of the corporate espionage scandal;

(b) if so, the details thereof;

(c) the number of Ministries and departments which may undergo such security vetting and the time by which the process is likely to be started and completed.

(d) whether study by the Indian Infosec Consortium has revealed that about 3,000 sensitive Government Computers had been compromised and their contents have been accessed through servers based in foreign countries; and

(e) if so, the details thereof and the reaction of the Government thereto?

Answer

MINISTER FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY
(SHRI RAVI SHANKAR PRASAD)

(a), (b) and (c): The Government of India has published Cyber Security Policies, 2010 for Government of India & Standard Operating Procedures for implementing Cyber Security Policies and circulated to all the Ministries and Departments for compliance and periodic verification of compliance:

(i) The security best practices, guidelines for protection of computer systems and cyber resources.

(ii) The security best practices and guidelines for protection of information contained in the computer system and cyber resources.

These policies aim at providing secure and acceptable use of cyber resources. It outlines security policy for users, system administrators, networks connected to Internet as well as security of cyber resources at the Ministries/Departments/Central Government and State Governments.

The compliance to these security best practices & guidelines and periodic verification of compliance in various Ministries/Departments of Government is a continuous process. These security best practices and guidelines apart from implementation of adequate security control measures include background verification of personnel in line with the perceived risks.

Further, the Government has also empanelled 51 auditors after following a stringent process which can be hired by Ministries/Departments for periodic verification of compliance and audit of the computer system and cyber resources.

(d) and (e): As per the guidelines of the Government, no sensitive or classified information is stored on computer systems connected to internet. All the classified/ sensitive information is dealt with as per the laid down guidelines and policies.

There have been unconfirmed media reports regarding the study by the Indian Infosec Consortium and compromise of sensitive Government computers for accessing their contents.

However, no such incidents involving compromise of sensitive government computers have been reported to the Indian Computer Emergency Response Team (CERT-In).

It is observed that there have been attempts from time to time to penetrate cyber networks and systems operating in Government. These attacks appear to be emanating from the cyber space of a number of countries around the world. The attackers compromise computer systems located in different parts of the World and use masquerading techniques and hidden servers to hide the identity of actual system from which the attacks are being launched.

In order to detect and prevent cyber security breaches, Government has taken several proactive measures as follows:

i) Government has released the "National Cyber Security Policy − 2013" for public use and implementation with all relevant

stakeholders. The objective of the policy is to create a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country.

ii) The Government, industry and other organizations are regularly strengthening their Information Technology infrastructure by installing devices and security controls to protect their infrastructure from such attacks.

iii) All the Ministries/ Departments of Central Government and State Governments have been asked to implement the Crisis Management Plan to counter cyber attacks and cyber terrorism.

iv) The Government has circulated Computer Security Policy and Guidelines to all the Ministries/Departments on taking steps to prevent, detect and mitigate cyber attacks. In addition, all state governments and UTs have been advised to implement appropriate security measures to prevent hacking of websites.

v) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis.

vi) The organizations operating critical information infrastructure are regularly advised to implement information security management practices based on International Standard ISO 27001. Ministries and Departments have been advised to carry out their IT systems audit regularly to ensure robustness of their systems.

vii) Cyber Security Mock Drills to assess preparedness of organizations to withstand cyber attacks are being conducted by the Government.

viii) The Government and industry are focusing on training their operations staff for protecting the infrastructure and handling incidents. The infrastructure w.r.t Cyber Forensics has been enhanced considerably.