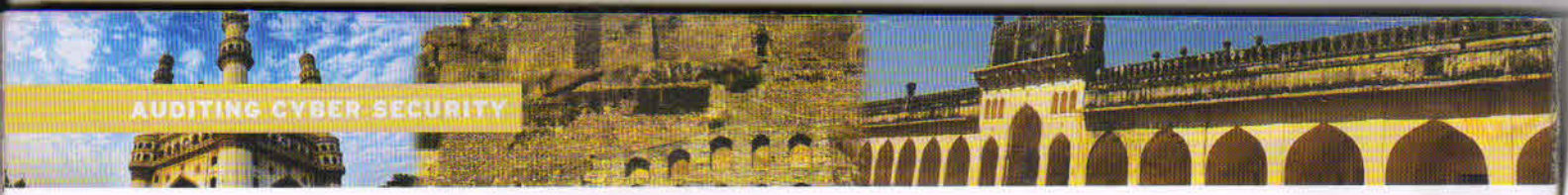

K P Sasidharan
Director General (WR)
Office of the Comptroller and Auditor General of India

EMERGING CYBER THREATS AND SECURITY ISSUES

It is difficult to ascertain the origin, identity or motivation of the perpetrators as they can operate with substantial impunity from virtually anywhere

The Ministry of Communications and Information Technology, Government of India, has recently released the National Cyber Security Policy (NCSP) "for secure computing environment and adequate trust and confidence in electronic transactions." The Information Technology (IT) infrastructure has, no doubt, emerged as the most critical catalyst for economic growth and prosperity, linking citizens into a virtually seamless fabric of interconnectivity, across physical and logical networks, going far beyond organizational and national boundaries. Good governance is possible only through reliable, secure and effective e-Governance.

The Indian IT sector has provided world-class technology solutions to help ensuring effective service delivery systems and economically viable powerful business solutions to emerging challenges. Realising the importance of IT sector, the Indian government at all levels – at the centre, states and the third tier government structure of Urban Local Bodies and Panchayati Raj Institutions has been adopting IT-enabled initiatives for improving citizen services, citizen identification, public distribution systems, healthcare through telemedicine, remote consultation, mobile clinics and outreaching people imparting education via e-Learning, virtual classrooms and similar innovative e-Solutions and financial service by providing mobile banking and payment gateways.

The government has adopted strategic National e-Governance Programmes (NeGP) and the Unique Identification Development Authority of India (UIDAI) programme with large scale IT backbone interlinking the nation to promote effective IT enabled solutions to various governance and service delivery issues. Considering the increasing internet vulnerabilities, abuse, cyber threats, terrorism, securing wireless and wired security of the computing environment and information systems, ensuring adequate trust and confidence in electronic transactions is a growing challenge world over. Creation of a reliable cyber information system with adequate security eco-system, in tune with globally networked online environment becomes an inevitable pre-requisite for the modern day governance.

A holistic dynamic and flexible cyber security strategy with constant vigil on updating in pace with emerging threats posed by technological trends is a must to safeguard the information systems and networks of the entire ICT users and service providers covering both government and non-government entities. While protecting the cyber space in the country, there should be a robust cyber security framework capable of addressing effectively the security related issues overa long period.

The Cyber Security Policy is intended for securing the cyber space considering its impact on national security, public safety and economic well-being. The cyber security needs are far beyond traditional technological measures like anti-virus, firewalls, placing anti-intrusion devices encompassing dynamic strategy designed to detect, stop and prevent attacks. For this reason, cyber security intelligence forms an integral component of security of cyber space to anticipate attacks and to adopt counter measures.

As stated in the government's policy statement it is important to have 'effective correlation of information from multiple sources and real-time monitoring of assets that need protection and at the same time ensuring that adequate expertise and process are in place to deal with crisis situations'. The policy should be geared to ensure security to people, process and technology while endeavouring to adopt the best available technological solutions with the help of adequately trained and qualified manpower.

Threats emanate from varied sources, target individuals, businesses, national infrastructures, and governments, posing significant risk for public safety, security of nations and the interconnected international Internet users as a whole. It is difficult to ascertain the origin, identity or motivation of the perpetrators as they can operate with substantial impunity from virtually anywhere. The motives include demonstration of technical know how, theft of money or information or even an extension of state conflict by criminals and potential terrorists or States themselves.

In the context of increasing sophistication and scale of criminal activity, all nations have to co-operate to prevent subversion of ICT supply chain. Inclusion of malicious malware in products and services erodes trust and affect national security. Cooperation among nations, private sector and civil society is indispensable to safeguard networks, computers, data bases, data centers and applications with proper security procedures and technological measures.

NCSP envisages in its scope of action cyber defense taking defensive actions against perpetrators of cyber crime on information systems by those who have political, economic motivation or who damage public safety and economic wellbeing of the society. The cyber defense system will be deploying technological capabilities for real-time protection and prompt incident response, driven by intelligence on the threat, directing, collecting, analysing and disseminating the relevant actionable intelligence information to the stakeholders concerned for

"The government needs to integrate competing interests to derive a holistic vision and plan to address the cyber security related issues to develop the policies, processes, people, and technology required to mitigate cyber security-related risks," says **K P Sasidharan**

proactive, preventive and protective measures. The effectiveness lies in ensuring resilience and continuity of operations. Creation of awareness on threats, conducive legal environment for taking appropriate counter measure, effective law enforcement, protection of IT networks and gateways and critical communication and information infrastructure, cyber security emergency response and resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.

Policy, promotion and enabling actions for compliance to international security best practices and conformity assessment product, process, technology and people andincentives for compliance.Indigenous development of suitable security techniques and technology solution oriented research and deployment of secure IT products and processes. Creation of a culture of cyber security for responsible user behaviour and actions; effective cybercrime prevention and prosecution actions; proactive preventive and reactive mitigation actions to reach out and neutralise the sources oftrouble and support for creation of global security eco system, including public-private partnership arrangements, information sharing, bilateral and multi-lateral agreements with overseas CERTs, security agencies and security vendors.

The objectives of NCSP are prevention of cyber-attacks, reducing vulnerability and enhancing the defense capability of critical ICT infrastructure. Minimising damage and recovery in a reasonable time frame time are the key drivers. It is vital significance to identify and classify critical information infrastructure facilities and assets and preparing roadmaps for organisation-wise security policy implementation in line with international security best practices standards and other related guidelines. Security threats and vulnerability assessments are monitored and use of secure products and services, protocols and communications, trusted networks anddigital control systems are to be ensured. Internet Service Providers (ISPs) will have to cooperate to secure information flow through their networks and gateways and appropriatelegally enforceable agreements will be set in place to support law enforcement, information security incident handling and crisis management processes on a 24x7 basis.

At national level, CERT-In, DIT will act as a nodal agency and co-ordinate all matters related to information security in the country,

with clearly defined roles and responsibilities. Emergency preparedness and crisis management will be strengthened through Mirror Centres, hot/warm/cold sites,communication, redundancy, and disaster recovery plans, test and evaluation of plans. Periodic and random verification of the level of emergency preparedness will be undertaken. Development of comprehensive repair and maintenance policy is essential to minimise falsealarms and increase cyber resource availability to all users efficiently. Along with tactical and strategic analysis of cyber attacks and vulnerability assessments, expanding the Cyber Warning and Information Network to support, it important to have prompt response by the government in coordinating crisis management for cyberspace security.

criminals to steal hundreds of millions of dollars and nation-states and other entities to steal intellectual property and sensitive military information. The government needs to integrate competing interests to derive a holistic vision and plan to address the cyber security related issues to develop the policies, processes, people, and technology required to mitigate cyber security-related risks. Cyber security policy includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions

"GOOD GOVERNANCE IS ONLY THROUGH RELIABLE, SECURE AND EFFECTIVE e-GOVERNANCE"

NCSP will be giving adequate importance to safeguard important wings of government like Defence, Energy, Finance, Space, Telecommunications, Transport, Public Essential Services and Utilities, Law Enforcement and Security are to be protected from large-scale defacement and semantic attacks on websites, Malicious code attacks, Large scale SPAM attacks, Spoofing, Phishing attacks, Social Engineering, Denial of Service (DoS) and Distributed DoS attacks, attacks on DNS, Applications, infrastructure and Routers, Compound attacks and High Energy RF attacks.

Implementation of Information Security Best Practices based on ISO 27001standard, Business Continuity Plan, Disaster Recovery, Security of Information and Network, Security Training and Awareness, Incident Management, Sharing of information pertaining to incidents and conducting mock drills to test the preparedness of Critical Security legal framework and a sound legal framework and effective law enforcement procedures are essential in deterring cyber-crime.

The architecture of the Nation's digital infrastructure, based largely upon the Internet, is not secure or resilient. Digital infrastructure has been suffering intrusions that have allowed as they relate to the security and stability of the global information and communications infrastructure.

A recent technical report on '2013 Information Security Breaches Survey ' conducted by PWC in association with Info-security Europe finds out that security breaches reach highest ever levels in UK businesses with increasing average cost of breaches. Attackers include criminals, hacktivists and competitors leading to multiple failures in people, processes, and technology. Consequently security budgets are increasing. Weaknesses in risk assessment and shortage of skilled manpower to tackle the threats and attacks become one of the key reasons.

In this context, it is important to note 'The Ten Steps' the UK government had specified in its guidelines to business on how to protect themselves from cyber security threats. These tens steps are information risk management, user education and awareness, home and mobile working, incident management, managing user privileges, removable media controls, monitoring, secure configuration, malware protection, network security. As technology is rapidly changing, there is a need to have a flexible cyber security policy, assigning adequate priority, investment, right attitude and security culture with extra care to keep pace with changing environment taking into account notorious malware kits like Blackhole and attacks arising out of Java in browser, vulnerability of passwords, increasing use of smart phones, tablets and social media platforms like Facebook, Twitter, and emerging risks arising out of adoption of cloud computing services.

There should be effective measures to detect incidence of different types of security breaches like infection by viruses and malicious software leading to systems failure and data theft, fraud and corruption; incidents caused by staff and outsiders with impact of breaches on business disruption, total cost of breach including financial loss and damage of reputation and an appropriate contingency plan for disaster management.

A comprehensive IT security should be reducing the attacks by monitoring malware and threats like vulnerabilities, applications and spam; ensuring users are protected irrespective of the place and device they use covering mobile gateway and cloud technologies; looking beyond antivirus signatures to detect risk behaviour and appearance of malicious codes; and constantly training and updating the skills of IT staff to effectively check the increasing new forms of attacks with complete visibility and granular control of the security system. In order to safeguard the business, it is important to assess the entire landscape of the cyber security, establish a baseline of current cyber security capabilities and identify the general training needs for the workforce.

As part of the Cyber Security Policy, a national nodal agency at apex level known as National Information Board (NIB) with members from relevant departments and agencies will be entrusted with information security and coordination for all strategic, military, government and business security requirements. There will be National Crisis Management Committee to address major crisis incidents, National Cyber Response Centre, National Information Infrastructure Protection Centre, National Disaster Management Authority, Standardisation, Testing and Quality Certification (STQC) Directorate will have to be in place and effectively manage cyber security related issues to safeguard cyberspace and information communication technology (ICT) devices and networks of the nation as envisaged in the much acclaimed policy statement.