Building an Information Security Infrastructure - A Comprehensive Framework towards a Robust, Resilient and Dependable Infrastructure

Shashi Ranjan, Manoj Kumar Maurya, Apurva Krishna Malviya, Rohit Yadav, Rahul Gupta, Madhvendra Mishra, Shashikant Rai

Department of MSCLIS and MBA-IT, Indian Institute of Information Technology, Allahabad, Uttar Pradesh 211012, India

Abstract

India is striving to become a knowledge economy by the year 2020. In order to achieve this goal, there is a growing focus both at the government level as well as private sector level to leverage the expertise of the IT and ITES sector of the country which has become one of the main drivers of growth for the Indian Economy. This has lead to increasing investment in IT infrastructure. In this paper we review this trend and analyze the importance of Information Security Infrastructure for the country. We propose a comprehensive conceptual framework for building a robust, resilient and dependable Information Security Infrastructure which will help in establishing India as the secure and trusted hub of the future.

Keywords: *Information Security Infrastructure, Information Security Management, Government Security Policy.*

1. Introduction

The growth of Indian IT Sector during last two decades has been nothing short of phenomenal. It has changed the way business is done in the country and has also paved the way for economical, societal and cultural changes.

IT has become one of the most significant growth catalysts for the Indian economy. Apart from fuelling India's economic growth, this sector has also contributed directly and indirectly to the various socio-economic parameters such as employment, standard of living and diversity among others. The sector has played a significant role in transforming India's image to that of a global player in providing world-class technology solutions and business services. [1]

The Indian IT industry has grown from a mere US $ 150 million in 1991-92 to a staggering US $ 58.8 billion (including over $46.3 billion worth of software exports) in 2008-2009. [2]

Notwithstanding the global recession, the Indian IT sector is expected to continue to be one of the sunshine sectors of the Indian economy showing rapid growth and promise.

According to a NASSCOM-McKinsey report titled 'Perspective 2020: Transform Business, Transform India', the exports component of the Indian industry is expected to reach US$ 175 billion in revenue by 2020. The domestic component will contribute US$ 50 billion in revenue by 2020. Together, the export and domestic markets are likely to bring in US$ 225 billion in revenue, as new opportunities emerge in areas such as public sector and healthcare and as geographies including Brazil, Russia, China and Japan opt for greater outsourcing. [3]

Moreover as Government tries to leverage the IT Infrastructure in providing public services to its citizens by means of various projects under National e-Governance Plan (NeGP), the need to build a robust Information Security Infrastructure becomes even more urgent.

2. Critical Information Infrastructure & Information Security Infrastructure

Leveraging the power of the Internet along with Information and Communication Technology (ICT) has made it possible to share vast amount of knowledge and information. This is driving all round socio-economic changes and growth throughout the country.

In this scheme of things, e-Infrastructure has become the key enabler for any knowledge society. E-Infrastructure comprises tools, facilities and resources that are needed for advanced collaboration and includes integration of various technologies such as the Internet, computing power, bandwidth provisioning, data storage etc.

Critical Information Infrastructure comprises of those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of the government or the economy. [4]

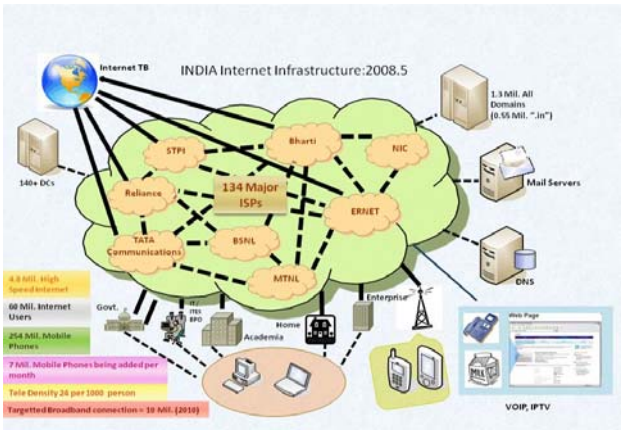

Fig.1 Internet Infrastructure in India Source: CERT In, 2008

3. Information Security Landscape

As more and more nations around the world are realizing the immense opportunities that IT can provide for their and their citizens benefits there is an unprecedented race to integrate their economies to the Internet economy. This stems from the fact that IT (including the Internet) is increasingly being seen not only as a means for expanding economic and business avenues but also offering ease of operations and outreach for Government's social welfare schemes.

3.1 Trends in Indian IT Sector

To With the advent and proliferation of distributed social networking technology (Facebook, Twitter etc.) in doing business, the trinity of - connectivity, complexity and extensibility - has added another dimension to the security landscape.

Although IT has been a great enabler in bringing economic prosperity and societal change, it has also increased the attack surface of the country for people with malicious intent. This challenge is not a local phenomenon but a global one – one that the world is becoming increasingly aware of.

3.2 Attack trends – Domestic and Global

Websense Global Threat Intelligence report on the global attack trend presents a clear picture of the recent trend in IT attacks as depicted in the following figures. Figure 2 details crime ware attacks and Figure 3 shows phishing trends globally over the last year. [5]

The map clearly indicates a gradual move of the Security landscape towards crime ware which includes cyber warfare between governments, industrial espionage and attacks against a nation's infrastructure. However in the Indian scenario phishing attacks have been more prominent.

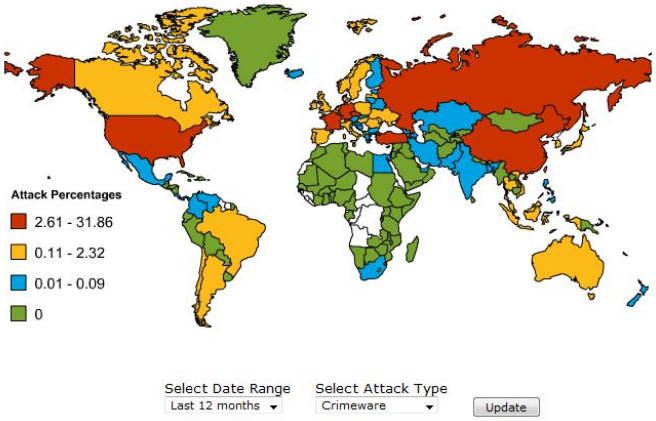

Fig.2 Crimeware Attack Trends 2011. Courtesy: Websense

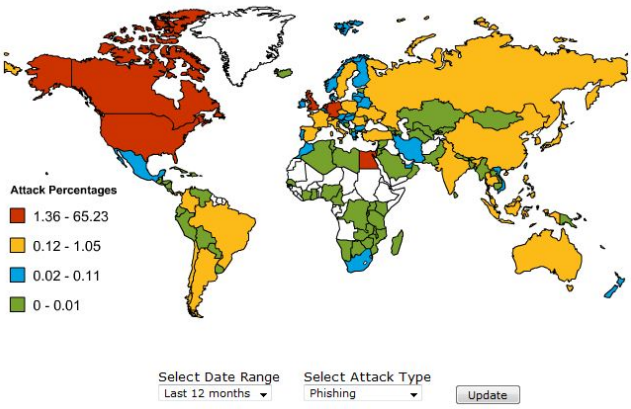

Fig.3 Phishing Attack Trends 2011. Courtesy: Websense

The annual report of CERT-In makes the security landscape of India clearer. Table 1 presents the summary of activities performed by CERT-In during the period 2006-2010.

As the table suggests, there has been a gradual increase in the number of incidents reported to CERT-In. This has coincided with the growth in the IT sector across India. As IT becomes more pervasive across India, the incidents and activities related to Information Security is bound to increase.

However, a recent report by PwC titled "Global State of Information Security Survey" shows that India has made major gains since 2006 with Information Security Practices and Safeguards. These have included hiring of CSOs and CISOs, implementing overall security strategy and using passwords.

However, India still reports higher rates of extortion, fraud, IP theft and financial losses than US.

Table 1: Summary of CERT-In Activities Courtesy: CERT-In

Security Incidents	2004	2005	2006	2007	2008	2009	2010
Phishing	3	101	239	392	604	374	508
Network Scanning / Probing	11	40	177	223	265	303	477
Virus / Malicious Code	5	95	19	358	408	596	1817
Spam	-	-	-	-	305	285	981
Website Compromise & Malware Propagation	-	-	-	-	835	6548	6344
Others	4	18	17	264	148	160	188
Total	23	254	552	1237	2565	8266	10315

**CERT-In stands for the Indian Computer Emergency Response Team. It acts as the nodal agency for responding to computer security incidents as and when required*

4. A Framework to Building an Information Security Infrastructure

India has a vision of transforming herself into a knowledge superpower by 2020. IT has the most prominent role to play in fulfilling this vision as outlined in the National IT Policy and the National Cyber Security Policy. This requires the need for robust, secure and scalable IT and Information Security Infrastructure build up.

In broad terms, any Government can play an active role in building up such an infrastructure, or can choose to be a passive player interfering only if substantial risks are at stake.

Government sector has enabled increased IT adoption in the country through sectors reforms that encourage IT acceptance and National programs such as National e-Governance Programs (NeGP) and the Unique Identification Development Authority of India (UIDAI) program that create large scale IT infrastructure and promote corporate participation. This has lead to another dimension in the Information security landscape in the country where the Government has started playing an active role as one of the drivers as well as facilitator in the Information Security field.

We now propose a comprehensive framework to build a robust, resilient and dependable Information Security Infrastructure for the country. (Refer Figure 4)

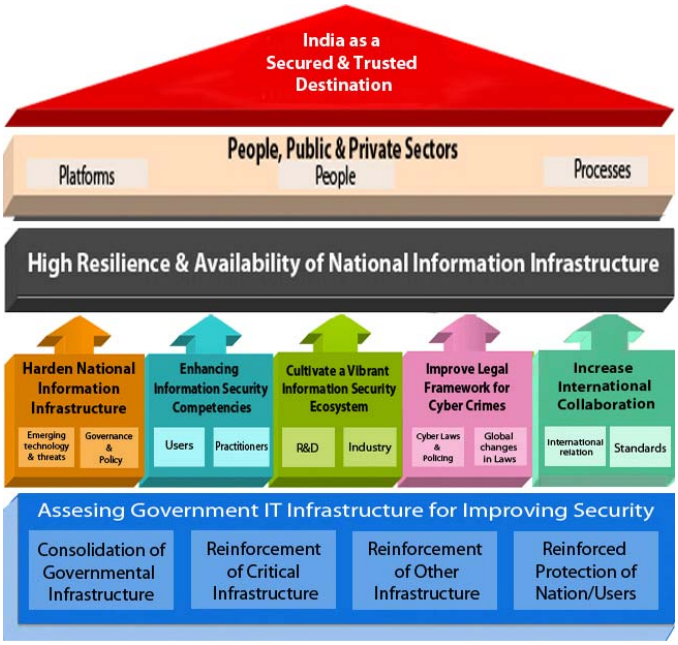

Fig.4 Proposed Framework for a robust, resilient & dependable Infrastructure Building

L1. Assessing Government IT Infrastructure for improving security

This has various sub-processes involved which are listed below:

a. Consolidation of governmental infrastructure
   - ❖ Establishment of a nodal agency responsible for information infrastructure auditing.
   - ❖ Regular audit of governmental infrastructure to assess gaps.

b. Reinforcement of critical infrastructures
   - ❖ Organization and dissemination of Safety Standards.
   - ❖ Improvement of critical infrastructure protection measures.
   - ❖ Elaboration of Business Continuity Plans.

c. Reinforcement of other infrastructures
   - ❖ Ensuring the IPv6-related information security.
   - ❖ Promoting safe electronic trading.
   - ❖ Ensuring information security in medical and education fields.

d. Reinforced Protection of the Nation/Users
   - ❖ Conducting an information security campaign.
   - ❖ Promotion of data protection for individual users.

L2. Improving Information Security Capability of IT

Infrastructure

This deals with the process of enhancing the information security related capabilities of the underlying Information Technology Infrastructure:

a. Harden National Information Infrastructure (NII)
   - ❖ Emerging technology & threats
     - ✓ Increasing dependency on ICT in socioeconomic activities.
     - ✓ Adapting to new technological innovations.
     - ✓ Globalization & NII.
   - ❖ Governance & Policy
     - ✓ Establishment of Information Security Governance Framework.
     - ✓ Establishment of a Counteractive Cyber Organization.
     - ✓ Establishment of policies adapted to changes in the information security environment.
     - ✓ Establishment of Proactive Information Security Measures

b. Enhancing Information Security Competencies
   - ❖ Users
     - ✓ Establishment of a three dimensional policy comprehensively covering the viewpoints of national security, crisis management, and nation/user protection.
   - ❖ Practitioners
     - ✓ Establishment of an information security policy that contributes to the economic growth strategy.
     - ✓ Cultivation of Information Security Human Resources.

c. Cultivate a Vibrant Information Security Ecosystem
   - ❖ R&D
     - ✓ Strategic furtherance of information security research and development.
   - ❖ Industry
     - ✓ Alliance between public and private sectors
     - ✓ National Association of Software and Service Companies (NASSCOM)
     - ✓ Data Security Council of India (DSCI)

d. Increase International Collaboration
   - ❖ International relation
     - ✓ Reinforcement of international alliances against cyber attacks through Computer Emergency Response Team (CERT) and other agencies.
     - ✓ Sharing of the cyber attack information with other countries.
     - ✓ Strengthening alliances with the US, EU, ASEAN, and other countries.
   - ❖ Standards
     - ✓ Review of the Standards for Information Security Measures for Central Government Computer Systems such as ISO/IEC27001:2005 and other relevant standards.
     - ✓ Promotion of secure encryption usage in government agencies.
     - ✓ Determining appropriate information security for the common number system for AADHAAR (UIDAI) and PAN (IT department).

e. Improve legal framework for cyber crimes.
   - ❖ Cyber Laws & Policing
     - ✓ Increasing awareness about the Information Technology (Amendment) Act, 2008.
     - ✓ Organization of a cybercrime policing infrastructure.
   - ❖ Up gradation of laws as per Global changes in the Cyber Security Landscape.
     - ✓ Identify measures to improve cyberspace safety and reliability.
   - ❖ Comparison of information security legal systems of different countries

L3. High Resilience & Availability of National Information Infrastructure

This process can be used to ensure that the NII is able to detect any cyber threats that can compromise nation's ability to provide a conducive environment to the fledging IT industry by taking timely and prudent corrective as well as preventive actions. This can be done by ensuring that the various stakeholders (refer Table 2) involved are taken into confidence and are encouraged to work in a collaborative manner.

L3. People, Public and Private Sectors

Indian IT scene has three chief stakeholders – people, the Government and the Private sector. Any framework has to accommodate the viewpoints of all three.

In order to do so we are in support of PPP model i.e. Public Private Partnership. The capabilities and expertise of various agencies such as NASSCOMM and DSCI can be leveraged to ensure these.

Table 2 Stakeholders in India's Information Security Infrastructure.

S.No.	Name Of Agency	Head	Responsibilities
01	National Information Board (NIB)	National Security Advisor	• Enunciating the national policy on information security and coordination
02	Ministry of Home Affairs (MHA)	Home Minister	• Ministry of Home Affairs issues security guidelines from time to time to secure physical infrastructure. • All matters related to internal security.
03	Ministry of Defense	Defense Ministry	• Deal with all aspects of Information Assurance and operations. • It has also formed the Defense CERT where primary function is to coordinate the activities of services/MoD CERTs. • It works in close association with CERT-In to ensure perpetual availability of Defense networks.
04	National Cyber Response Centre - Indian Computer Emergency Response Team (CERT-In)	Ministry of Communications and Information Technology	• CERT-In monitors Indian cyberspace and coordinates alerts and warning of imminent attacks and detection of malicious attacks among public and private cyber users and organizations in the country. • It maintains 24x7 operations centre and has working relations/collaborations and contacts with CERTs, all over the world • It works with Government, Public & Private Sectors and Users in the country and monitors cyber incidents

**Compiled from Department of IT, GoI website*

NASSCOM is the industry association for the IT-BPO sector in India. A not-for-profit organization funded by the industry, its objective is to build a growth led and sustainable technology and business services sector in the country.

The 4E initiative of NASSCOM for the outsourcing industry for promotion and enforcement of security relies on Engagement with all stakeholders involved, Education of service providers, Enactment to create a policy environment, Enforcement of standards and constant checks.

DSCI, a section 25 not-for-profit company, was setup as an independent Self Regulatory Organization (SRO) by NASSCOM, to promote data protection, develop security and privacy codes & standards and encourage the IT/BPO industry to implement the same. DSCI has developed Best Practices for Data Protection that is in line with global standards and cover emerging disciplines of security and privacy. [6]

Taking cue from these agencies the Government can collaborate with the people and the industry to actively shape a secure and trusted future for nation's Information Infrastructure.

5. Recommendations

Apart from the proposed framework, following recommendations can be helpful to this end:

a. View cyber security not as an optional issue but an imperative need of the hour.
b. Make long term investments in capacity building, R&D and Infrastructure to facilitate next-generation security solutions.
c. Encourage Public-Private partnership to leverage India Inc's globally recognized expertise in the field.
d. Decrease foreign dependency on countries like China by encouraging capacity building for hardware sector.
e. Implement security best practices in Government organizations and critical sectors such as assigning CISOs, preparing a security plan, implementing appropriate controls etc.
f. Conducting audit of Information Infrastructure on a periodic basis.

6. Conclusion

Recent spur in cyber attacks, identity theft and financial frauds against the IT infrastructure has highlighted the importance of securing the cyber space. As India becomes more prominent in global affairs, fast-shifting trends in both technologies and threats make it likely that the security issues of the IT infrastructure will only intensify in the coming years.

Due to the geographic location of the country and the hostility that it faces from its neighbors, India needs to be fully prepared for the next wave of proxy wars that will be unleashed upon its cyber territory.

Although recent surveys show India making considerable gains in this field a lot is still to be desired. With a comparatively young population that is increasingly becoming tech-savvy, it is imperative that we are ready to face the challenges head on. Any Government has the responsibility of providing security for its citizens against various threats including that of the cyber world. As more and more people start using and relying on the IT infrastructure, it is imperative that India rises to the challenge in order to secure a brighter future.

References

[1] Department of Information Technology (2011) *National Cyber Security Policy.* New Delhi [Online] [Accessed on 05 January 2012] Available from: www.mit.gov.in/sites/upload_files/dit/files/ncsp_060411.pdf

[2] *Indian IT-BPO industry shows resilience; to grow by 4-7 percent in FY09-10 (2010) [Online] [Accessed on 08 January 2012]Available from: http://www.nasscom.org/Indian-IT-BPO-industry-shows-resilience-to-grow-by-4-7-percent-in-FY09-10-57224*

[3] NASSCOM-McKinsey (2009) *Perspective 2020: Transform Business, Transform India* New Delhi: NASSCOM.

[4] Radhakrishnan, R. and Radhakrishnan, R. (2004) *IT Infrastructure Architecture Building Blocks [Online] [Accessed on 20 February, 2012] Available from: The Open Group. http://www3.opengroup.org*

[5] WEBSENSE *Attack Information Center Websense Global Threat Intelligence* (2012) [Online] [Accessed on 15 February, 2012] Available from:

http://securitylabs.websense.com/content/CrimewarePhishing.aspx

[6] Data Security Council of India (2012) *About Us [Online][Accessed on 20 February, 2012]Available from: http://www.dsci.in/taxonomypage/1*

[7] The National Science Foundation US (March 2007) *Cyber infrastructure Vision for 21st Century Discovery. Virginia [Online] [Accessed on 15 February, 2012] Available from: http://www.nsf.gov/pubs/2007/nsf0728/*

[8] US-CERT (2005) *The National Strategy to Secure Cyberspace* [Online] [Accessed on 20 February 2012] Available from: United States Computer Emergency Readiness Team http://www.us-cert.gov .

[9] Peltier, T. et al. (2003) *Information Security Fundamentals.* 1st ed. Auerbach Publications.

[10] Harris, S. (2010) *CISSP All-in-One Exam Guide.* 5th ed. McGraw-Hill Osborne.

[11] Cole, E. (2009) *Network Security Bible.* 2nd ed. Wiley.

Shashi Ranjan is a Master's Degree (MS) student in Information Security & Cyber Law at the Indian Institute of Information Technology, Allahabad (UP, India). He has an engineering degree in Information Science & Engineering from the Visvesvaraya Technological University, Belgaum (Karnataka, India). His research interests include Information Security Policies, Risk Management and policy issues.

Manoj Kumar Maurya is a Master's Degree (MS) student in Information Security & Cyber Law at the Indian Institute of Information Technology, Allahabad (UP, India). He has an engineering degree in Computer Science & Engineering from the Uttar Pradesh Technical University, Lucknow (UP, India). His research interests include cryptography and information security issues.

Apurva Krishna Malviya is a Master's Degree (MS) student in Information Security & Cyber Law at the Indian Institute of Information Technology, Allahabad (UP, India). He has a graduate degree in Commerce from the University of Allahabad, Allahabad (UP, India) and Law from Awadhesh Pratap Singh University, Rewa (MP,India). His research interests include information security compliance and cyber laws.

Rohit Yadav is a Master's Degree (MS) student in Information Security & Cyber Law at the Indian Institute of Information Technology, Allahabad (UP, India). He has an engineering degree in Computer Science & Engineering from the Uttar Pradesh Technical University, Lucknow (UP, India). His research interests include computer forensics and risk management.