CYBER GOVERNANCE

[1]Rishab Jain, [2]Lalit Garg, [3]Nivedita Shah, [4]Prof. Gurpreet Kaur
[1,2,3]Students, [4]Assistant Professor
Department Of Computer Science
Mahavir Swami Institute of Technology, Sonipat, Haryana

Abstract: - Under the leadership of Mr. Narender Modi, India is actively promoting the Digital India campaign and India is inviting companies from around the world to come to India and establish their network here in India. This campaign comes with a lot of security concerns related to the country. This article argues about how to deal with these issues by highlighting the major problems and giving them a solution.

We all know that now a days cyber crimes are increasing with fast rate this is because we all are going digital for our every need from buying a underwear to buying gold and these all things require some links from our private information, mainly our bank account details and at that the user is very scared to enter them but he/she also want to be a part of this revolution which is changing our lives in day to day manner. This fear give birth to the thief's which we cannot see, touch or feel and these are the most dangerous ones as we don't know when and where they are going to attack and this is not only for an individual but these things also attacks nations, countries as they have the databases of all the people present in this universe and they have every small details of them. By seeing such difficulties in the cyber space. Some governments took some steps to prevent these causes. With the introduction of United Nations Commission on International Trade Law (UNICITRAL) model law on e-commerce in 1996 (United Nations, 1996), several jurisdictions adopted focused law to regulate online commerce and related e-govemance. The Indian parliament enacted its Information Technology Act, 2000 to incorporate essential provisions of UNICITRAL model law on e-commerce. This statute primarily catered to four basic needs, i.e., to recognize online transfer of data, to formulate a basic framework for e-govemance, creation of framework for strengthening cyber security, and amending the existing laws including Indian Penal Code, Indian Evidence Act, Bankers Book Evidence law etc. for updating the traditional criminal laws in order to support the penology related to cyber security.1 The 2000 version of the Information Technology Act was soon challenged by an enormous growth of information communication technology and criminalities in cyber space. The statute fell short of providing protection of data including sensitive personal data, addressing issues related to growth of e-commerce (Basu & Jones, 2003), crimes targeting women and children (Haider & Jaishankar, 2008), and cyber terrorism (Haider, 2011).

Countries including the United States of America, United Kingdom etc. had revamped their laws including cyber security policies post the 9/11 attacks (Collin, 1996; Trachtman, 2009; Wykes & Harcus, 2010). After the 26/11 Mumbai Taj Hotel attack, it was understood that the existing Information Technology Act, 2000 proved to be extremely weak for addressing cyber warfare and cyber terrorism (Haider, 2011). Even though Indian parliament had already framed a new Bill in 2006 to address data security including e-commerce, e-govemance, and criminalities including cyber terrorism and cyber warfare, it could not provide much hope as cyber security experts assessed the inability of the Bill to address issues which it promised to address. The Bill therefore was revamped and in 2008 the new amended version of the Information Technology Act was implemented.

This amended Act emphasized economic fraud, e-service delivery, e-govemance, and cyber terrorism: in short, it tried to holistically address cyber security aspects." To execute the provisions of this law, several rules were introduced, including:

(1) electronic service delivery
(2) reasonable security practices and procedures and sensitive personal data or information, intermediary guidelines
(3) procedures and safeguards for interception, monitoring, and decryption of information
4) procedures and safeguards for monitoring and collecting traffic data or information
(5) procedures and safeguards for blocking for access to information by the public.

The Information Technology)' Act (IT Act) 2000 (amended in 2008) addressed electronic governance in chapter III, which included a discussion on legal recognition of electronic records and signatures, legal recognition of the use of the same by Government and its agencies, e-service delivery by sendee providers, retention of electronic records, auditing etc.

1. E-GOVERNANCE IN INDIA: EMERGING TRENDS

E-government is organizing public management in order to increase efficiency, transparency, accessibility and responsiveness to citizens through the intensive and strategic use of information and communication technologies in the inner management of the public sector (intra and inter-governmental relations) as well as in its daily relations with citizens and users of public services.

E-governance is an ICT-enabled tool to achieve good governance. We may think of it as integrated governance. Since it integrates people, processes, information, and technology in the service of achieving the aim of good governance. Indian government has been using IT for more than 40 years. So what's new about e-governance? What's new is that we are moving on from IT to ICTs and from IT to IS.

2. E-GOVERNANCE: MAJOR CHALLENGES IN INDIA

Poor people and poor infrastructure are major challenges in countries like India. It poses a major challenge in reaping the full benefits of service provision under e-
ISSN: 2278 – 7798 All Rights Reserved © 2014 IJSETR
governance. follows:

The various barriers can be enumerated as

2.1 Poverty: Accessing Internet is a costly affair for the poor who struggle for their livelihood in developing countries like India. Required infrastructure in the form of installing the necessary telephone lines needed for internet or email access is equally unaffordable in most poor countries.

2.2 Technical illiteracy: There is general lack of technical literacy as well as literacy in countries like India.

2.3 Language Dominance: The dominance of English on the internet constrains the access of non-English- speaking population. In the case of India, 95 percent of the population does not speak English. Due to such overwhelming dominance of English over these communication channels, computers and the internet are quite useless in Indian villages.

2.4 Unawareness: There is general lack of awareness regarding benefits of E-Governance as well as the process involved in implementing successful G-C, G-G and G-B projects.

2.5 Inequality: Inequality in gaining access to public sector services between various sections of citizens, especially between urban and rural communities, between the educated and illiterate, and between the rich and poor.

2.6 Infrastructure: Lack of necessary infrastructure like electricity, internet, technology and ways of communications will affect the speed which delays the implementation.

2.7 Impediments for the Re-Engineering process:
Implementation of E-Governance projects requires lots of restructuring in administrative processes, redefining of administrative procedures and formats which finds the resistance in almost all the departments at all the levels

3. REASONS OF SUCCESS OR FAILURE OF E-GOVERNMENT PROJECTS IN INDIA

An estimated US$3 trillion was spent during the first decade of the 21st century on government information systems. Yet recent studies suggest between 60 to 80% of e-government projects fail in some way leading to "a massive wastage of financial, human and political resources, and an inability to deliver the potential benefits of e-government to its beneficiaries". Systems failures are recognized as occurring from a complex interaction of technical and human factors set in a social situation rather than as the result of the failure of one particular component (human or technical) [5].
If we take the view that an e-government project has failed if it misses any of the criteria that are implicit in such a common-sense definition of success, then it is hardly surprising that most projects are categorized as failures. But to understand failure, we need to examine the basis on which academic writers, who generally adopt an informative stance to evaluation, decide to provide descriptive and diagnostic information on the projects being considered. These diagnostic approaches fall into three main categories – factoral analyses, systems approaches and interpretive studies. Heeks (2002) applied a factor-based approach to an analysis of the significant number of failures in e-government projects. A survey of relevant case studies in the literature led him to the identification of seven dimensions necessary and sufficient to measure the gap that exists between 'current reality' and the 'design concept' of the intended application. He contends that the wider the gap that exists on each of these dimensions, the higher the risk of failure for the project.
The seven dimensions of potential design-reality gaps to be explored on an e-government project are summarized by the ITPOSMO acronym and are outlined as:

I. Information: the formal information held by the digital system and the informal information used by the people involved with the system.

II. Technology: mainly focuses on the digital IT but can also cover other information-handling technologies such as paper or analogue telephones.

III. Processes: the activities undertaken by the relevant stakeholders for whom the e- government system operates both information- related processes and broader business processes.

IV. Objectives and values: often the most important dimension since the objectives
component covers issues of self-interest and organizational politics, and can even be seen to incorporate formal organizational strategies; the values component covers culture: what stakeholders feel are the right and wrong ways to do things.

V. Staffing and skills: covers the number of staff involved with the e-government system, and the competencies of those staff and other users.

VI. Management systems and structures: the overall management systems required to organize operation and use of the e-government system, plus the way in which stakeholder agencies/groups are structured, both formally and informally.

VII. Other resources: the time and money required to implement and operate the e-government system.

It is a common knowledge that majority of e- Government projects have failed to yield the potential benefits that are otherwise possible with deployment of ICT in public sector. There are enough surveys carried out on e-Government projects which tend to conclude that many e-Government projects fail to achieve the intended objectives / benefits. Failure rate is high amongst developing countries.

Governments are increasingly under pressure to ‗showcase' successful projects! The failure of a vast majority of e-Government projects in developing countries including in India raises important and serious questions about the justifiability of the huge investments in financial and human resources being made in these projects.

4. E-GOVERNMENT PROJECT MANAGEMENT: ISSUES AND CHALLENGES IN INDIA

E-Government is recognized internationally as an enabler toward achieving good governance, reducing cost of operations for the government, and increasing the ability of citizens and businesses to access public services in an effective and cost efficient manner. The successful implementation of e-Government project is a challenging task.

4.1 Some current challenges for managing E- Government Projects in India

A. Lack of effective project management tools and methods.

B. Absence of proper planning, various ad hoc tasks are taken up by the project team due to which the focus on critical activities is lost.

C. The knowledge of project management concepts is very low in Government officials forming part of the e-Government Project team.

D. E-Government projects do not follow any standardized project management implementation frameworks.

E. Resources are over loaded with work due to inadequate staffing. Sometimes tasks not assigned to the team appropriately.

F. No control of central IT agencies during project execution. The decision making process is generally left to individual line ministries and departments since funding comes from them.

G. No provisioning of Project Management dashboard for collaborative project monitoring by all stakeholders in large e-Government projects.

H. Inadequate tracking of how the project is being implemented, tasks causing delays.

I. No monitoring of Cost and Schedule at project checkpoints.

J. During the project initiation, the baseline data is not captured which is useful for bench marking of activities.

REFERENCES

1. https://ebrary.net/173518/political_science/cyber_governance_data_protection_india_critical_legal_analysis

2. https://link.springer.com/chapter/10.1007/978-981-16-9128-7_3

3. https://link.springer.com/chapter/10.1007/978-3-030-50244-7_10

4. https://scholarlypublications.universiteitleiden.nl/handle/1887/48177