International Journal of Latest Trends in Engineering and Technology
Special Issue SACAIM 2016, pp. 484-489
e-ISSN:2278-621X

Study on the need for Cyber Security & Cyber Hygiene in e-Governance Framework in India

Namratha Sharath[1], Pallavi[2] and Prof Santhosh Rebello[3]

Abstract- Electronic Governance(e-gov) is a valuble tool in the hands of Indian govenment to deliver public services effiecently.This presentation focuses on the need for Cyber Security & Cyber Hygiene in E-Governance. Though this issue is of very much imporatance, Cyber security for e-Governance projects of India is still not contemplated by Indian Government. Therefore it is neccessary to primarily cover grounds on the security that needs to be built around the application softwares that is built to give the governance an online presence without any potential threat of being rigged. Particularly now, that the world is witnessing an explosion in the number of threats that are associated with the increased proliferation of different technologies,hence cyber security is paramount. Identification of the areas that are prone to attacks and then create an environment to quarantine such incidents is very important. The ecosystem for cyber security and data protection necessitates a strong legal framework, proactive government initiatives, active involvement of, and contribution by the industry and effective law enforcement mechanism. Data privacy plays an important aspect of this conceptual topic, but setting up the usual firewall might set limitations on transparency of E-Governance soltions to benifit all its facets. For now relying upon Indian e-Governance services,baring a few exceptional ones, is risky proposition and could be avoided.

Keywords- Cyber Security, Network Security,Brainstorming

I. INTRODUCTION TO E-GOVERNANCE, CYBER SECURITY AND CYBER HYGIENE.

Electronic Governance has already profoundly changed many tedious processes with the introduction of different E-governance plans. Though E-governance is seen to be very citizen friendly, the applications are usually hosted in public domain which makes it unguarded to security breaches. Henceforth, various procedures, processes and practices that involve protecting networks, computers, online devices and data from attack, damage or unauthorized access, that is Cyber-Security[2] becomes very essential.

Imagine a software that helps the election scenario, where citizens are perceived as clients and customers. Availing them to vote even from home with no much afford using their citizen ID also aiding them with analysis reports about different candidates according to their credentials and display reports and ratings that suggest how successful the respective candidate can be as a politician. Now even a small breach over the Internet also known as cyber-attack could intensively affect the whole election results. So how can we decide upon various areas of compliance to be considered to avoid such cyber-attacks, henceforth maintaining one's safety over the Internet? This process could involve daily routines, occasional checks to maintain the cyber hygiene.[5]

[1] *School of Information Technology, AIMIT, Mangalore, Karnataka India*
[2] *School of Information Technology, AIMIT, Mangalore, Karnataka India*
[3] *Dean, Department of IT, AIMIT, Mangalore, Karnataka India*

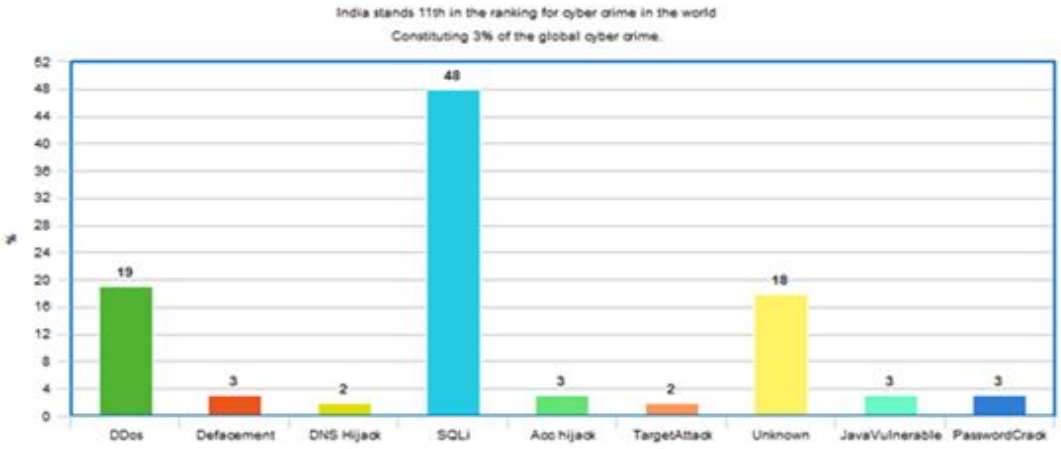

Figure : Risks of potential attacks

Risk analysis: Various kinds of qualitative or quantitative methods, such as analysis, comparison, evaluation, etc. are done to decide the importance of every factor for e-governance risks, rank the factors, and then evaluate possible result to implement the e-governance systems. Threat is a kind of potentiality which is launched.Unintentionally by threat source attacking the vulnerabilities of the system. If a system has vulnerabilities, threat sources become risks. So in the process of risk analysis, we must identify and describe threat sources. To identify threats the system is facing, we can use different methods, such as brainstorming, Scenarios Analysis, etc.

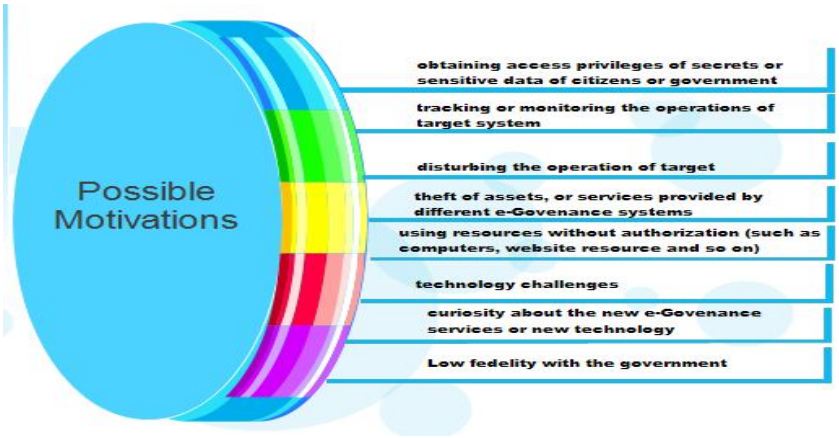

Figure: Threats from people with possible motivations are listed above

Though clear standards like ISO 27001 and ISO 20000[7]for IT services and security management are presently being used by varied e-Governance applications but few concerns are still not addressed. With the increase in multiple players and agencies becoming highly involved in e-Governance initiatives, not only standards but also putting in place a cyber-security framework to e-Government in India has become essentially important to ensure end-to-end security to various e-Governance services.[1]

A breach of security could lead to lost opportunities, defamation, loss of goodwill, repudiation loss, financial loss, transactional loss, loss of citizens confidence and many others.

II.E-GOVERNANCE SENARIO IN INDIA.

E-Governance can be defined as use of the information and communication by the government to enhance the range, quality of information and services provided to citizens in the cost affective manner with the ability to transform relations with citizens businesses and other arms of the government.E-Governance can transform citizen service to enpower citzens,by providing access to the information as well as enabling their participation in government to enhance citizen economic and social oppornituties.

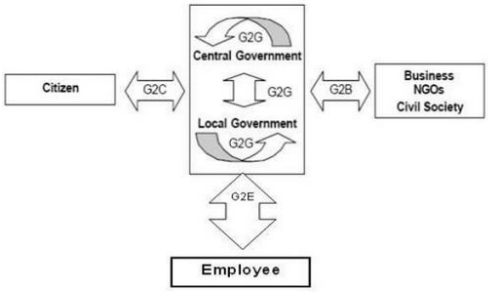

Figure: Type of interactions

The National e-Governance Plan (NeGP) is an initiative of the Government of India to make all government services available to the citizens of India via electronic media.[8]NeGP was formulated by the Department of Electronics and Information Technology (DeitY) and Department of Administrative Reforms and Public Grievances (DARPG).

Better access of information and quality services for citizens with the expand reach of governance could be implemented with e-Gov.Due to lack of intergrated services, lack of key persons, population and diversity languages e-Govenance faces major drawbacks in India.

Though India is the largest democracy in the world with the need for effective and transparent public governance, it stood at 118th position in the recent UN E-Government Survey 2014 with an E-Government Development Index (EGDI) of 0.3834. As per the Survey results, Online Service Index (OSI), Telecommunication Infrastructure Index (TII) and Human Capital Index (HCI) for India were 0.5433, 0.1372 and 0.4698 respectively. India has performed very poorly in the UN E-Government Survey 2014. India should make more solid efforts to make the e-Governance projects more effective to provide her citizens efficient, effective and transparent access to public services that the citizens deserve.[12]

III. E-GOVERNANCE FRAMEWORK SECURITY CURRENT FRAMEWORK

The emergence of Information and communications Technology (ICT) has provided means for faster and better communication, efficient storage, retrieval and processing of data and exchange and utilization of information to its users, be they individuals, groups, businesses, organizations or governments

With growing computerization and increasing internet connectivity, this process has presently reached a stage where more and more users are motivated to modifying their ways of doing things in order to leverage the advantages provided by ICT. In other words, this has led to ‘business process re-engineering’.[6]

This would generally involve the use of ICTs by government agencies for any or all of the following reasons:

(a) Exchange of information with citizens, businesses or other government departments
(b) Speedier and more efficient delivery of public services
(c) Improving internal efficiency
(d) Reducing costs / increasing revenue
(e) Re-structuring of administrative processes
(f) Improving quality of services.

E-governance applications of various departments ensure security of data and privacy protection through the following measures[4]

- Network security (NIPS, Firewalls, content filtering, HIPS, antivirus, etc.)
- Data security (robust SAN environment with high raid levels to prevent any data loss)
- Application security (audited by empanelled TPA)
- DR/BCP provisioning (real-time data is replicated to DR site in case of any physical calamity or damage to resources at primary site, backup exists at remote different seismological locations) [3]
- Cloud security (There are several Organisations/consortia actively involved in the development of security standards/ guidelines.Different Cloud Security Framework/Guidelines being developed by several consortia/organizations).

A. Framework for better e-governance security

A new set of Security Control Principles called e-Government Security Matrix (EGSM) is based on the security Control Principles described by Vic (J.R.) Winkler [3] as well as other industry standard Frameworks like ISO 2001, Cloud Control Matrix (CCM), NIST SP 800-144.It consists of four Security Control domains as following:

1.Foundational Security Domain
- Security policy - policy, principles guidelines, procedures and standards
- Security in Cloud service providers (CSP) Operations and Management
- Security requirements for third party providers.
- Security awareness and training for personal

2.Deep Defence Domain
- Identification of Federated, Privileged and business access management and control.
- Security of Service Delivery Model
- Application & Software Assurance and Maintenance
- Security of Host & VM
- Network Security Management
- Wireless Security Management
- Cryptographic Control & Key Management

3.Operational Security Domain
- Physical access management & Environment Security
- Assets Control Management
- Assets Control Management
- Security Incident Management
- Operation Practices like media and memory protection, security function isolation

4.Business requirement Domain
- Business Continuity Management with Backups & Contingency Planning
- Legal Audit & Compliance

- Audit assurance and compliance with third party audits
- Resource planning

B. Activities involved in improving cyber security

1. Information on data accessed can be communicated on real time basis using ICT tools
2. Advice states in setting up new security infrastructure. For example, it is proposed to set up e-Gov security operation center (SOC) as part of NII 2.0. [7]
3. Indelible audit trail using encrypted flat file
4. Advice states on security enhancement of the e-Gov infrastructure that have been setup for e-Gov service delivery.
5. Advice states in implementing the e-Gov security policy and the detailed procedure documents that have been prepared.
6. Prevent server intrusion and data theft upfront rather than do post-mortem analysis.
7. Communication and cooperation with industry to understand new security products , conduct concept proofs for products that can be used in strengthening the security posture of e-Gov infrastructure and then advice the states on the same.
8. Capacity building in cyber security for states. [5]

IV. CHALLENGES IN THE E-GOVERNANCE SERVICES IMPLEMENTATION WITH RESPECT TO SECURITY ISSUES.

Third party involvement.

Today the technology has grown significantly but the advancement is not in-sync with the human resource available when concerned about the technical skills. Important concern for government today is limited internal technical skills available, which introduces the third-party vendors.Public Private Partnership(PPP) could lead to security concerns likevulnerabilities caused by defective specification, design, and implementation.[1]

Sharing of data across various e-Governance implementations

`Though e-Governance today could be a single window access to various government services like Election Confidential(ELECON).This is achieved by the seamless data sharing across applications.

Multiple locations and delivery channels.

As the e-Governance applications are very resource intensive. It is normally spread across multiple locations and delivery channels for information retrieval and dispatch. Hence multiple ports for information breaching is possible.

Access Controls and securitynot made very comprehensive.

Lack of adequate knowledge and understanding on various management controls on standards by department, policies not made comprehensive, the controls in the International standards need to be made more prescriptive as per hour requirements.[9]

V. AWARENESS AND ASSESSMENT

Study of new Security practices

Study of best practices on security includes those worked out by STQC, DSCI and CERT-IN and adopting /modifying them into e-Governance Security Framework.

Identification of security elements

An e-Governance service should be able to identify the security elements right from conceptualization to analysis, design, implementation and post implementation stages.

Mechanism for Prevention of cyber-attacks

Evolve processes and procedures for setting up the mechanism to prevent cyber-attack or incidents and then implement the same.

Capacity building

Creates awareness and building capacity in the area of Information security in e-Governance in India.

Ensuring security could be achieved by preparation of detailed procedures covering technology and processes for e-Gov. [1]

VI. CONCLUSION

E-Governance has already started to occupy significant role in the global and economy. Various agencies provide huge support in e-government initiatives. Essentially, actions for securing information and information systems are required to be done at different levels in the E-Governance. Along with transparency in functioning greater change in the data protection, computer crimes and hosting of services from procurement to service delivery is highly suggested.

It's not just the government that carry forward with their actions but besides them PPP, network services providers (ISP), large businesses and small users/home users are also required to play their part to enhance the security of cyber space within the country.
While designing projects, the government usually thinks about security of the system, but not privacy of the data. Security in the minds of the government is achieved only through strengthening infrastructure.

REFERENCES

[1] Saxena, K. B. C. (2004) Towards excellence in e-Governance. In Towards E-Government: Management Challenges, M P Gupta (Ed.). Tata McGraw-Hill, India

[2] RenuBudhiraja, Challenges and Role of standards in Building interoperable e-Governance Solutions

[3] Vic (J.R.) Winkler,Securing the Cloud: Cloud Computer Security Techniques and Tactics(ElsevierInc, 2011,ISBN: 978-1-59749-592-9)

[4] Allen, Julia. "Security Is Not Just a Technical Issue." Build Security In web site, Department of Homeland Security, October 2006.

[5] T. D. Susanto and R. Goodwin, "Factors Influencing Citizen Adoption of SMS-Based e-Government Services," Electronic Journal of E-Government, Vol. 8, No. 1, 2010, pp. 55-71.

[6] F. V. Morgeson, D. Van Amburg and S. Mithas, "Misplaced Trust? Exploring the Structure of the e-Government-Citizen Trust Relationship," Journal of Public Administration Research and Theory, 2010.

[7] Rao, V. R. (2013). A framework for unified digital government: A case of India. Journal of E-Governance

[8] Steven H. Spewak& Steven C. Hill, Enterprise Architecture Planning: Developing a Blueprint for Data, Application and Technology, John Wiley & Sons, New York, ISBN 0-471-599859