International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 08 | Nov-2015 www.irjet.net p-ISSN: 2395-0072

A case study on Cyber Security in E-Governance

Kumar D[1], Dr. N. Panchanatham[2]

[1] PhD Research Scholar in Management, Karpagam University, India
[2] Professor, Department of Business Administration, Annamalai University, India

---

Abstract - ***E-Governance is the outgrowth of the efforts made by the governments to improve relations with their citizens. If certain conditions are fulfilled, the legal value of electronic transactions shall be equivalent to that of other forms of communication, such as the written form. To protect E-Governance projects there is a need for information security best practices. Security polices, practices and procedures must be in place as well as utilization of security technology, which help to protect e-Government systems against attack, detect abnormal activities services and to have a proven contingency plan in place. Fundamental factors are to have a proper public-key infrastructure providing required level of authentication and integrity and also to have a continuous awareness and training program to ensure people understand security threats, know how to identify potential issues and behave accordingly to maintain a secure e-Government service. This paper stretches its objectives for classification of user communities for Governance and obligation of each community in Cyber security promoting the Governance with Information and Communication Technology as a case study.***

Key Words: *Cyber Security, E-Governance, Information Technology Act*

INTRODUCTION

E-Governance is the outgrowth of the efforts made by the governments to improve relations with their citizens. With its ingrained transparency and openness, given the principles of Internet, E-Governance brings governments more closely to their citizens. Therefore, E-Governance has a larger social angle, as it ensures a more wide and representative democracy. In a knowledge economy, competitive advantage relies on the capability to adapt to the changing environment by the continuous generation and application of new knowledge (Kumar and Panchanatham, 2014a). Many businesses cannot even function without the use of Information and Communication Technology (ICT) in their operations (Kumar and Panchanatham 2014b).

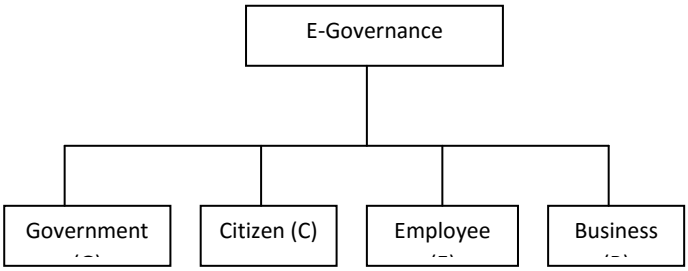
The cyber law is the law governing the acts that happen in the intangible digital world such as giving a legal status to the intangible information in the cyber space, security and privacy of such information, crimes relating to the damages caused to or by the cyber information and so on. The cyber laws are significant and valid for regulating cyber matters. Security is mainly about safeguarding the ICT assets of any organization or framework. The assets could be internal or external such as data, information, knowledge resources, programs, hardware, networks and so on. The threat to security of ICT systems may be from many sources and in different forms. Some of the internal sources of threat in e-governance are the employees of private or public agencies, customers or end users of the e-governance programs. The external sources of threat are the hackers, criminal/terrorist groups or organizations, intelligence and investigating agencies. Threats to the assets may be of different types and of varying intensities and impact values.

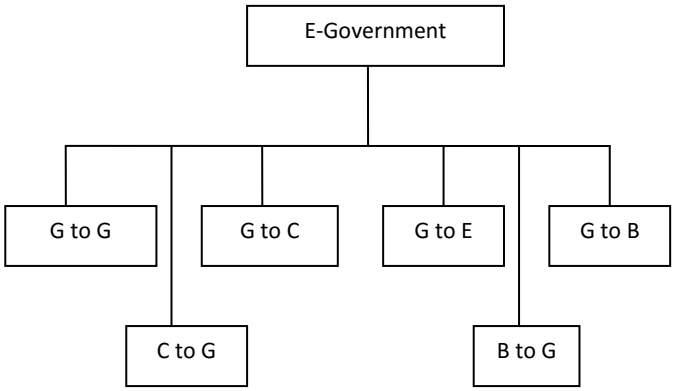
Existing and potential threats in the sphere of cyber security are among the most serious challenges of the 21st century. Threats emanate from a wide variety of sources, and manifest themselves in disruptive activities that target individuals, businesses, national infrastructures, and governments alike. Their effects carry significant risk for public safety, the security of nations and the stability of the globally linked international community as a whole. Malicious use of Information Technology can easily be concealed. The origin, identity of the perpetrator, or motivation for the disruption can be difficult to ascertain. Often, the perpetrators of these activities can only be inferred from the target, the effect or other circumstantial evidence. Threat actors can operate with substantial impunity from virtually anywhere. The motives for disruption vary widely, from simply demonstrating technical prowess, to the theft of money or information, or as an extension of state conflict. Many malicious tools and methodologies originate in the efforts of criminals and hackers. The growing sophistication and

scale of criminal activity increases the potential for harmful actions.

CLASSIFICATION

Managing E-Governance therefore means managing a large portfolio of divergent responsibilities in a coherent manner with all the subjects that comprise in the E-Governance implementation and usage. In order to develop an E-Government system, all the users using the system should be known. Illustration below depicts a schematic representation of explicit classification of the E-Government communities and their application viz. the Government, Citizen, Employee and Business which have their inter-linked process in some activities. For example, most of the E-Governance activities are targeted to the Citizens either directly or indirectly which is one of the inter linking. All the communities and directly possible interlinked E-Governance activities are given below.





The illustration above gives a layered approach for the integration of E-Governance services and promoting them with a legal reform. As shown above the transformation involves four communities and six outcomes with these four communities. The main objective is to have E-Governance with sustainable development in all these outcomes.

DISCUSSION

There are various models globally to implement the Electronic Governance in each sector. The above illustration reveals that there are differing communities and outcomes on the usefulness and credibility of the existent tools. Cyber security is the activity of protecting information and information systems (networks, computers, data bases, data centers and applications) with appropriate procedural and technological security measures. In that sense, the notion of cyber security is quite generic and encompasses all protection activities. Cyber defense relates to a much more specialized activity linked to particular aspects and organizations. The distinguishing factors between cyber security and cyber defense in a network environment are the nature of the threat, the assets that need to be protected and the mechanisms applied to ensure that protection. Cyber defense relates to defensive actions against activities primarily originating from hostile actors that have political, quasi-political or economic motivation that have an impact on national security, public safety or economic well being of the society. The cyber defense environment requires deployment of technologies and capabilities for real-time protection and incident response. This paves the way for interoperability and for creation of ICT systems that conform to the new regime of the joined up government.

Public-private partnership is a key component of cyber security in E-Governance. These partnerships can usefully confront coordination problems. They can also significantly enhance information exchange and cooperation. The public private engagement will take a variety of forms and will address awareness, training, technological improvements, vulnerability remediation and recovery operations. These actions will help in leveraging rapid technological developments and capabilities of the public sector.

Increasingly, States across the globe are concerned that the Information and Communication Technology (ICT) supply chain could be influenced or subverted in ways that would affect normal, secure and reliable use of Information Technology in various applications. Inclusion of malicious hidden functions in the Information Technology can undermine confidence in products and services, erode trust in commerce, and affect national security. As disruptive activities using Information Technology grow more complex and dangerous in the cyber space, it is obvious that no State is able to address these threats alone. Confronting the challenges of the present and future trend depends on successful cooperation among like-minded partners. Collaboration among States, and between States, the private sector and civil society, is important and the effectiveness of measures to improve cyber security

requires broad international cooperation.

APPLICABILITY

In accordance with the E-Governance challenges and obstacles the critical success factors in the E-Governance have to be investigated. From the process view, high security, standardization and knowledge management are a must of E-Governance, followed by the provision of specific services and its quality. Assuring security of cyber space requires careful and due attention to creation of well defined systems and processes, use of appropriate technology and more importantly, engaging right kind of people with suitable awareness, ethics and behavior. Considering the transnational character of the Information Technology and the cyber space, the technical & legal challenges in ensuring security of Information, Information Systems & Networks as well as related impact on socio-economic life in the state, the priorities for action for creating a secure cyber eco-system include series of enabling processes, direct actions and cooperative & collaborative efforts within the state and beyond, which covers the following:

• Creation of necessary situational awareness regarding threats to Information and Communication Technology (ICT) infrastructure for determination and implementation of suitable response.

• Creation of a conducive legal environment in support of safe and secure cyber space, adequate trust & confidence in electronic transactions, enhancement of law enforcement capabilities that can enable responsible action by stakeholders and effective prosecution.

• Protection of IT networks & gateways and critical communication & information infrastructure.

• Placing 24 x 7 mechanisms for cyber security emergency response & 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) and incentives for compliance.

• Indigenous development of suitable security techniques & technology through frontier technology research, solution oriented research, proof of concept, pilot development etc. and deployment of secure IT products/processes

• Creation of cyber security influenced culture for responsible user behavior and actions.

• Effective cyber crime prevention & prosecution actions in all the ICT applicable environments.

• Proactive preventive & reactive mitigation actions to reach out & neutralize the sources of trouble and support for creation of global security eco system, including public-private partnership arrangements, information sharing, bilateral & multi-lateral agreements with applicable overseas state agencies, security agencies and security vendors etc.

• Protection of data while in process, handling, storage & transit and protection of sensitive personal information to create a necessary environment of trust.

Top-level management of government departments or agencies should pay attention to the development of suitable Information Security policy and guidelines and encourage the use of appropriate technology and applications in the organization. In order to ensure implementation security best practices in critical sector organizations and periodic verification of compliance, there is a need to create, establish and operate an 'Information Security Assurance Framework'. This framework is aimed at assisting combined efforts of all applicable groups in protecting critical information infrastructure.

CONCLUSION

E-Governance has already occupied a significant place in the global economy. Various agencies of United Nations Organization (UNO) and the World Bank 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. According to Kumar and Panchanatham (2015b), the Government needs to be transparent in its functioning and for the same it needs to introduce legislation if required. E-Governance requires a range of legislative changes including electronic signatures; electronic archiving; data matching; freedom of information; data protection; computer crime; and intellectual property rights legislation. Regulatory changes are required for a host of activities from procurement to service delivery. According to Kumar and Panchanatham (2015a), it is the responsibility of the State to bring in sufficiently strong legislation to discourage and put down the misuse of the Internet and other cyber media for any nefarious activities. Besides the actions by Government, other stakeholders such as 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. This paper has discussed about the legal requirements of Cyber Security in providing a comprehensive E-Governance initiative. More research is needed at this stage and in future to design the required infrastructure that are built around the digital advancements and the E-Governance vision and policies.

REFERENCES

[1] Cyber Laws (n.d) Retrieved December 31, 2013, from http://indianrailways.gov.in
[2] E-Governance (n.d) Retrieved December 31, 2013, from http://en.wikipedia.org/wiki/E-Governance
[3] Holmes (2003). "Solutions come to those who wait". Times of India. May 20
[4] J. Satyanarayana (2006). E-Government. Prentice Hall India.
[5] Kajikawa (2008). Research core and framework of sustainability science. Sustainability Science, 3(2), 215–239. doi:10.1007/s11625-008-0053-1.
[6] Kumar D and Panchanatham N (2014a). Strategies for Rebooting the Government in e-Mode, Global Journal for Research Analysis, Aug 2014, Vol 3 Issue 8.
[7] Kumar D and Panchanatham N (2014b). Strategies for Effective E-Governance Management, International Journal on Global Business Management & Research, Aug 2014, Vol 3 Issue 1.
[8] Kumar D and Panchanatham N (2015a). A study on Cyber law in promoting E-Governance, AE International Journal of Multidisciplinary Research, May 2015
[9] Kumar D and Panchanatham N (2015b). Enforcing Transparency in Indian E-Governance Through ICT, International Journal of Business Management & Research, Jan 2015
[10] National Cyber Security Policy (n.d) Retrieved December 31, 2013, from http://deity.gov.in
[11] Saxena, K. B. C. (2004) Towards excellence in e-Governance. In Towards E-Government: Management Challenges, M P Gupta (Ed.). Tata McGraw-Hill, India