Implementation of E-Governance projects: Development, Threats & Targets

Harmeet Malhotra[1], Dr. Ruchira Bhargava[2], Dr. Meenu Dave[3]

doi: 10.5958/2347-7202.2017.00009.3

ABSTRACT

eGovernance is, in essence, the application of Information and Communications Technology to government functioning with the goal of ushering transparency and accountability for its services, improved efficiency within various institutional bodies and improvement in interface with business and industry. This would generally involve the efficient usage of ICTs by various government agencies for exchanging information with citizens, businesses or other government departments, quick and orderly delivery of public services, refining internal efficiency, reducing costs / increasing revenue and re-structuring of administrative processes and enhancing quality of services.

This paper discusses the eGovernance project development and implementation issues along with threats they are exposed to. There are various threat actors/ agents that can lead to the loss or breach of confidential data and e-resources of government departments and other business organizations. The various types of intentional and unintentional threats have been further discussed along with their major targets that can disrupt the services and transaction of these projects.

KEYWORDS

eGovernance, Cyber Security, Threats, Cyber Attacks

1. INTRODUCTION

The aim of e-Governance is to make the communication between government and citizens (G2C), government and business enterprises (G2B), inter-agency relationships (G2G), etc more friendly, easier, transparent, and cheaper. eGovernance is being promoted through a centralized initiative to the extent necessary to ensure citizen-centric orientation, to realize the objective of inter-operability of various e-Governance applications and to ensure proper use of ICT infrastructure and resources allowing decentralized implementation model. The aim is to also identifying successful projects and replacing them with required customization if required. According to international organization, UNESCO, "Governance refers to the exercise of political, economic and administrative authority in the management of a country's affairs, including citizens' articulation of their interests and exercise of their legal rights and obligations. E-Governance may be understood as the performance of this governance via the electronic medium in order to facilitate an efficient, speedy and transparent process of disseminating information to the public, and other agencies, and for performing government administration activities". [1]

In any software or system, the main regions that can be attacked are programs, peripherals, communication channels and input/output. These attacks can be active or passive. In case of active attacks the intruder may change the original content that is being transferred whereas in passive attack it only listens to the content and do not change it. The information security threats are generally related to authentication, privacy,

[1]*AssociateProfessor,Institute of Information Technology & Management,(Affiliated to GGSIPU),NewDelhi*
Email: harmeet_hello@yahoo.com
[2] *Professor, SJJT University, Rajasthan*
Email:ekhvaabs09@gmail.com
[3]*Professor, Jagannath University, Jaipur*
Emai: meenu.dave@jagannathuniversity.org

This journal is cited as : **JIMS 8i-Int'l J. of Inf. Comm. & Computing Technology(IJICCT)**

authorization, integrity and non-repudiation. Authentication is defined as the process that ensures and confirms the identity of the user. Authorization is the function of specifying access to resources related to information security and computer security in general and to access control in particular. It is normally preceded by authentication for user identity verification.[3] Non-repudiation means the method of guaranteeing that the message transmitted between two parties contain the digital signatures of the sender and later on nobody can deny that the message has not been sent by them. The case of receiving and email from a sender who denies that he is the sender is the case of non-repudiation. Integrity ensures the accuracy and consistency of the data even after the modification by the authorized. Many applications stores the personal data of the users such as their bank details, financial details, medical records, etc that should not be disclosed and privacy of such information should be fully maintained.

2. OBJECTIVES

1. To study various obstacles in implementation of eGovernance projects.
2. To find out various threat agents to eGovernance projects.
3. To study the major target areas of threat agents.

3. eGOVERNANCE PROJECT DEVELOPMENT LIFE CYCLE

The process of development of these projects is somewhat different from other software development process. In other words we can say that SDLC is an integral part of eGovernance Life Cycle model. The eGLC focuses more on business and stakeholders needs and priorities whereas SDLC model focuses on technical artifacts and process related aspects of the software such as software design, development, implementation management

As per **National Institute for Smart Governance**[7], the key stages of developing eGovernance projects are as follows:

eGovernance Strategy Development - The development of eGovernance projects requires a clear vision and objective and formulating a proper strategy for implementation. First stage requires proper need assessment of the project along with identification of institutional structures & capacities for implementation.

Current State Assessment - Secondly an in-depth assessment of business functions and services identified for coverage under e-Governance project must be performed. The current approach for performing business functions and delivering services must be studied and scope of improvement must be identified. The current systems (IT) implemented in the department should be studied and the gaps should be properly analyzed. The stakeholders need must be understood and good practices from similar projects in similar domains must be studied.

Future State Definition - The next step would be to define how the identified business functions and services shall be performed going forward to cover all the areas of improvement. This stage defines the new business processes. The capacities and skillset required along with the IT infrastructure and funding must be assessed. An enterprise architecture covering application, data, network, security, data center architecture should be framed.

Implementation approach and sourcing - Next, a road map of development & implementation should be prepared including development of Business Model, RFP Development, and Vendor Evaluation and Selection. The detailed implementation plan has to be prepared, project investment and cost should be evaluated, and vendor identification and evaluation reports must be prepared. Moreover, project monitoring,

tracking and evaluation plan should be finalized. All the related documents must be maintained.

Develop and implement IT system - The major activities of this stage are application software development, IT infrastructure creation, third party acceptance testing, project documentation and lastly training and capacity buildi 293 stage of development the project goes live.

Operate and sustain – This stage covers tasks related to system operations and maintenance, software change management and objectives & benefits evaluation and reinforcement.

4. IMPLEMENTATION ISSUE IN EGOVERNANCE PROJECTS

Implementation of e-Governance is a highly intricate process that requires networking, provisioning of hardware and software, process Re-engineering and change management. The obstacles or barriers in implementing these projects can be technological barriers, socio-cultural, legal and political barriers. There are various challenges in implementing projects such as significant investments, low return on investment, lack of stable project and permanent leadership with managerial powers to drive projects, lack of capacities to conceptualize and manage e-Governance projects, poor communication to the stakeholders and users on objectives and benefits, lack of capacities to conceptualize and manage e-Governance projects, inadequate resources for project (people and funding), minimal focus on project and systems quality assurance, etc.

Besides the external factors like political issues, management issues, organizational policies, etc, the technological factors also play a major role. The technological support to e-governance projects must ensure that the data and information maintained in the databases must be effective, confidential, available, and reliable and should also maintain the integrity of the same. There are various technological issues that if not taken into account may lead to failure of the project. The various technological obstacles involved are Integration of e-governance services among various departments, Communication gap among the development team or other stakeholders, the compatibility and compliance with management systems, records and work processes. The other problems can be inadequate IT infrastructure, lack of security and privacy, lack of training and knowledge transfer, lack of comprehensive policy, legal and regulatory framework, lack of legacy systems, etc.

5. OVERVIEW OF THREATS AGENTS/ INTRUDERS IN EGOVERNANCE PROJECTS

Intruders have can have different intentions that might be related to financial gain, influencing public opinion, espionage and so on. They can be individual attackers or a group of experts with sufficient knowledge and resources named as sophisticated attackers. It is quite difficult to list what motivates the hackers to attack the system. Generally they try to disrupt the government services, provide them financial loss, access media and news websites, military networks and so on. It is very difficult to estimate the impact of intrusion as it totally depends upon the goal to be achieved. Generally the intruders can be classified into internal and external. Internal intruders are part of the system and might have easy access & privilege to access the system whereas external intruders are the people that do not belong to the network domain.

Secondly, the intruders can be either individual hackers or organized group of people. Financial institutions are generally hacked by the individual hackers. Their bank details such as credit card number, etc are accessed and then used in buying goods and services. Public websites and social media websites are also one of the targets of individual intruders. They generally make use of tools such as viruses, worms, sniffers, etc to attack

or gain unauthorized access to the system. Intruders working inside the organization may also provide company's system related confidential to outside parties to exploit the vulnerabilities that can enable an attack. [4]

With the increase in usage of IoT technology, few criminal groups have also become very active. These groups are technology savvy groups and have sufficient funds, expertise and resources. They are very skillful at creating botnets and malicious software (e.g., computer viruses and scareware) and denial-of-service attack methods.[4] They generally target typical organizations for revenge, theft, economic espionage and even sell the confidential information such as financial data to terrorists or other criminal groups. The groups involved in cyber terrorism generally targets military systems, banks and other national organizations of religious and political interests, thereby affecting the economy of a country. There is another group of hackers named hacktivists that are engaged into the activities of DoS, fraud and identity theft.

These days intelligence agencies of from different countries are also becoming persistent in their efforts to probe the military systems of other countries for specific purposes such as industrial, political and military espionage [4]. They have huge technological infrastructure, lot many experts and research & development cell with sufficient funding that are totally involved towards various software related malicious acts and helps them in accomplishing their intrusion goals. The agencies are biggest threat to networks and necessitate tight scrutiny and supervise approaches to safeguard against threats to the information systems of utmost importance for any country and military establishment.[4]

Thus, hackers have the potential to compromise the confidentiality, integrity or availability of systems by their actions. Externally this action may manifest itself in website defacement, or theft of customer details. Persons on-site perhaps temporarily, who are visitors or bystanders may pose a risk, by observing information when present in the facility, or perhaps unauthorized access systems that are logged in. [6]

6. CYBER THREATS TO EGOVERNANCE PROJECTS

There are immense challenges posed on the IT department to fight against these vulnerabilities. The web servers, cloud, communication channels, etc all should be secure enough to fight against the harmful cyber attacks. Cyber security in terms of e-governance projects can be defined as an activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. The hacker who is an unauthorized user can attempt to or gain access to an information system bypassing the security mechanisms of a network.
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.

The threats in cyber security can be categorized into intentional and unintentional threats.

6.1 Unintentional Threats

Social engineering involves the manipulation of individuals to get them to unwittingly perform actions that cause harm or increase the probability of causing future harm, which we call "unintentional insider threat." [2]

Insider threat remains a major concern among computer and organizational security professionals, more than 40 per cent of whom report that their greatest concern is employees accidentally jeopardizing security through data leaks and or similar errors.[1]

The most common forms of accidental threats are caused by employee mistakes, frequently resulting from poor training and improper use of tools.

Possible results include unintentional damage to the system, modification or destruction of user programs or data, disclosure of sensitive information, or residual data that the user or management cannot find.

6.2 Intentional Threats

These threats can be brute force attack, social engineering attacks, cyber frauds, phishing, malware attacks, botnet attacks, vandalism, ransomware, session hijacking, etc.

Bot-net operators use a network of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. [3]

Few criminal groups seek to attack systems for financial gain. Specifically, organized criminal groups use spam, phishing, and spyware/malware to commit identity theft, online fraud and computer extortion.[3] International corporate spies and criminal organizations also pose a threat to the nations through their ability to conduct industrial espionage, large-scale monetary theft and to hire or develop hacker talent.

Hackers break into networks for varied reasons like thrill of the challenge, revenge, stalking, monetary gain and political activism. While gaining unauthorized access one requires a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. [3] The worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.

The disgruntled organization insider is a primary source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data.[3] The insider threat comprises of contractors recruited by the organization as well as careless or badly trained employees who may unintentionally inculcate malware into systems.

Phishers, individuals or small groups execute phishing schemes in an attempt to steal identities or information generally for monetary gain. Similarly, spammers can also distribute unsolicited e-mail with hidden or false information in order to sell products, conduc 295 schemes, distribute spyware or malware of attack organizations (e.g., a denial of service). They may also use spam and spyware or malware to accomplish their objectives. [3]

Cyber Terrorists tend to destroy, disable or expose critical infrastructures in order to threaten national security, can cause large number of casualties, weaken the economic system, and destroy public morale and confidence. They may use different phishing schemes or spyware/malware in order to gather sensitive information or generate funds. [3]

Attacks against users by producing and distributing spyware or malware are carried out by spyware and malware authors with malicious intent. Several destructive computer viruses and worms have harmed files and hard drives. [3]

Opportunities could be lost due to breach of security, defamation, loss of goodwill, repudiation loss, financial loss, transactional loss, loss of citizen's confidence ETC.

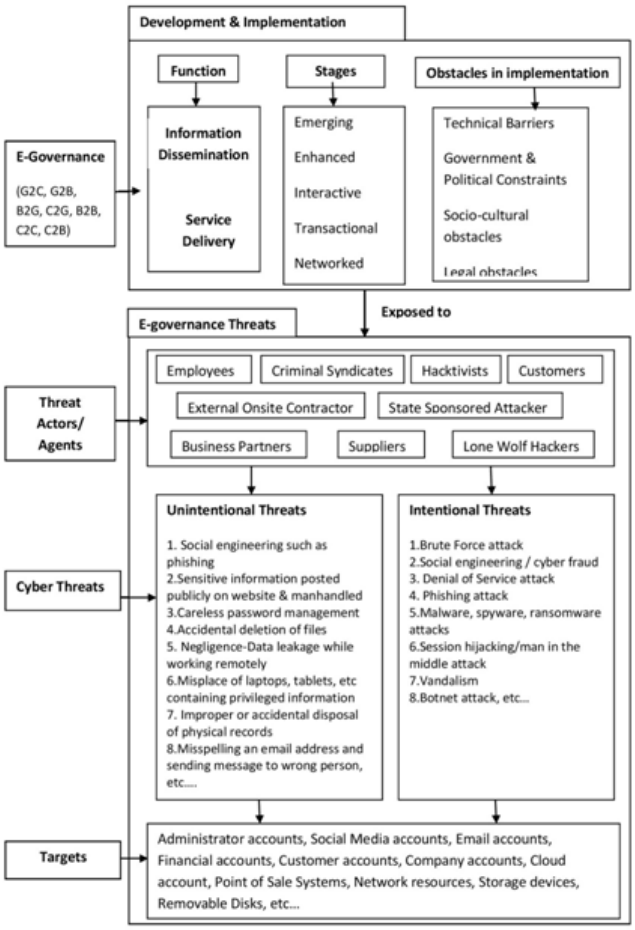

Figure: Conceptual linking of implementation, threat agents and their targets

7. TARGETS OF CYBER AGENTS

Generally, the targets of threat agents are administrative accounts, social media accounts, email accounts, financial accounts, company accounts, point of sale systems, network resources, storage devices, and removable disks and so on.

On the other hand, if the fraud is designed to extract money from an organization, it may affect both the organization and its customers or constituents. A criminal may be able to siphon significant amounts of money from organization's financial accounts before the activity raises suspicions and leads to financial loss also. Sensitive data may also be compromised if a criminal can access customer data, such as credit card information, he or she may be able to steal that information and use money mules to abuse the customers' financial or credit card accounts. Not only this, there can be damage to reputation in case an organization experiences any fraud they may lose the trust and loyalty of their customers or partners.

8. CONCLUSION

The lack of visibility of cyber security at board level and senior management is a common problem for security professionals within large organizations. A structured approach is required for safeguarding critical infrastructure against developing cyber-threats. It is required that the government aggressively collaborates with public and private sectors on a regular basis to prevent, respond to, and coordinate mitigation efforts against attempted disruptions and adverse impacts to the nation's critical infrastructure.

There should be well defined cyber security policies for developing secure eGovernance projects that would include preventive, protective, and mitigation measures to be taken. There must be well drafted recovery and contingency plans ready in case of any cyber fraud.

REFERENCES

[1] "Concept of e-Governance." Internet: http://vikaspedia.in/e-governance/national-e-governance-plan/concept-of-e-governance.

[2] Mundie David. "Unintentional Insider Threat and Social Engineering." Internet: https://insights.sei.cmu.edu/sei_blog/2014/03/unintentional-insider-threat-and-social-engineering.html, 2014.

[3] Iqbal Kauser Harhat Shahapur, Sheema Syeda, Guddadavar Asha (2015), A Survey on Different Modes of Wormhole Attack and it's Countermeasures in MANET, International Journal of Computer Applications Technology and Research Volume 4– Issue 5, 377 - 379, 2015, ISSN:- 2319–8656

[4] Mohamed Abomhara and Geir M. Køien. "Cyber Security and the Internet of Things: Vulnerabilities,Threats, Intruders and Attacks." Internet: https://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-1439_414.pdf, May 2015

[5] "Information Security Management in e-Governance." Internet: https://www.aphrdi.ap.gov.in/documents/Trainings@APHRDI/2017/4_Apr/Information%20Security%20Management/Day1%20-%20S4%20Introduction%20to%20Information%20Security%20in%20e-Governance.pdf

[6] "Cyber Security for SCADA Systems." Internet:https://www.thalesgroup.com/sites/default/files/asset/document/thales-cyber-security-for-scada-systems.pdf, 2013

[7] "Governance Capacity Building: e-Governance Project Lifecycle." Internet: http://meity.gov.in/writereaddata/files/e-Governance_Project_Lifecycle_Participant_Handbook-5Day_CourseV1_20412.pdf, April 2012

[8] "An overview on cyber security policy in India." Internet**:** http://www.thehansindia.com/posts/index/Civil-Services/2016-12-09/An-overview-on-cyber-security-policy-in-India/267807, Dec 2016

[9] "Cyber security: everybody's imperative, A guide for the C-suite and boards on guarding against cyber risks." Internet: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ers-cyber-security-everybodys-imperative.pdf

[10] "Cyber Security Policy 2017- Government of Haryana." Internet:http://www.haryana.gov.in/citizens/policies/Haryana%20state%20policy-2.pdf

[11] "Cybersecurity Strategy: a tool for better cyber protection." Internet: https://www.thegfce.com/news/news/2016/12/07/cybersecurity-strategy-a-tool-for-better-cyber-protection, Dec 2016

[12] Metivier Becky. "6 Steps to Cyber Security Risk Assessment." Internet: https://www.sagedatasecurity.com/blog/6-steps-to-a-cybersecurity-risk-assessment