E-Government, Open Data, and Security: Overcoming Information Security Issues with Open Data

Abdurakhmanov Abduaziz Abdugaffarovich, Varisov Akmal Abbasovich*, Nasrullaev Nurbek Bakhtiyarovich

Department of Information Security, Tashkent University of Information Technologies, Uzbekistan

1. Introduction

As nations begin to shift toward more information based societies, the implementation and use of information in technological and governmental systems has become increasingly more important. E-government represents a fundamental and necessary shift towards the implementation of these technologies and how we will better use information to improve the interactions between governments, citizens, and corporations.

Open data in E-government plays an important part in improving the overall interactions between all stakeholders in a society. The increased use of technologies to promote open data governments also brings along with it several factors that are concerning and need to be addressed. The security of our data and information, arguably the most important of those factors, is what we will address in this article. Understanding what e-governments are, how open government data is necessary to implement good governance in them, and what potential risks are posed to the security of our information should help us to properly address these issues and provide a guideline to resolve them.

2. E-government and Open Government Data E-government

The term E-Government is generally considered to be a very loose term. As defined by the United Nations and The American Society for Public Administration E-governance is:

“Broadly defined, e-government includes the use of all information and communication technologies, from fax to wireless palm pilots, to facilitate the daily administration of government. To which it may be added “that improves citizen access to government information, services and expertise to ensure citizen participation in and satisfaction with the government process”

E-government system is primarily intended for the convenience of citizens. In the development of the security of information resources and the creation of e–government developers missed elementary errors as to the management of the system and on the treatment of people in various public services.

E-government can also be considered as digital interactions between government and citizens (G2C), government and businesses (G2B), government to employees (G2E), as well as government and government agencies (G2G). This digital interaction consists of governance, information and communication technologies (ICT’s), business process re-engineering (BPR), and e-citizen’s at all levels of government (city, state/province, national, and international).

There are many different drivers for E-Government, and why it is necessary. Consider a cost effective and time efficient manner of delivering many government services. E-government also provides the possibility of enhanced bilateral communication channels and easier implementation of commercialization strategies. A well designed E-government system would also be able to incorporate cost recovery mechanisms to cover the maintenance, storage, and collection of information. There is a substantial amount of value in the information that is held by governments, and it should be put to use.

How to say have become global or continental e –
government entail integration of the nation, science, invention and economic growth (friendly) countries and many other important sectors of the government. And this government will provide one rapid pace.

E–government system is that all countries are very different. It differs essentially by three factors. These are:

1. Openness. Because of countries starting from the internal politics of many information resources can beat the open access can not beat.
2. From sources. Here an important role is played by the number of information resources and services provided.
3. Reliability. It is the accuracy of the information in the information resources plays an important role in the development of the e–government and ensure transparency of government. And this is for a secure economic growth, financial and social sectors of the state and of course will lead to trust the work of the state.

Namely, the above listed three factors create many problems for a global e–government. But it should be noted there is a fourth economic-financial factor which also plays an important role in the creation of a global or continental e–government. And this is the economic development of the state.

But the security of information resources in the global e–government connects only increases. Each country has its own certification organization and standardization. And they largely determine the policy and security architecture and what software will be used for the provision of services and security. Of course there are international standard organizations such as ISO and IEEE. But what standards or technology staff to ensure the security of information resources do not enjoy, the main thing that they are not contradictory to each other there. And by the standards and technical level.

Unfortunately, not all governments have adapted well to this new shift toward e-government. Issues such as:
- Information classification schemes (what type of information does a government want/need to publish, and how long should the information be retained)
- Where the information located (is it stored in a single repository or is it spread across multiple repositories?)
- How clean the information is (how was it checked, how was it collected?,; what security procedures were involved in processing the information?)
- What are the technological, managerial, and legal risks are there (in processing government held information)
- Data inconsistency (overlapping of data from multiple government sources)

have arisen from this rapid migration to e-government in the last 10 to 15 years. So the real question is, with the rapid development and implementation of e-governments all over the world, how can we avoid running into these problems?

3. Open Government Data and the Three Pillars

At the core of E-government lies open government, and open government data. Open government is often referred to as “a measure of governmental response to citizen’s demands for information and services from government organizations” (La Porte et.al. 2009). The two major components of open government consist of transparency and participation. Transparency generally refers to the extent of which information, decision-making processes, and policy activities of governments are publicly known to citizens. On the other hand, interactivity is primarily concerned with citizen participation and engagement, as well as the government’s responsiveness and democracy. These two basic elements are key components in the promotion of good quality governance.

According to research by the Division of Public Administration and Development Management (DPADM) UNDESA there are three pillars or dimensions in pursuing open government: policy and regulatory framework, organizational framework, and channels and modalities. Each pillar plays a unique role in establishing and sustaining open government. For example, the promotion of public information disclosure and increased transparency is reliant on developing the necessary legal framework to accompany such an initiative.

|                     | Transparency                      | Interactivity                  |
|---------------------|-----------------------------------|--------------------------------|
| **Policy and Regulatory Framework** | Freedom of Information Act | Citizen Participation Act |
|                     | Public Information Disclosure Act | Citizen Budget |
| **Organizational Framework** | Agencies in charge of public information disclosure | Agencies and courts |
| **Channels and Modalities** | Offline meetings | Public hearings |
|                     | Online channels such as Internet, social media, mobile channels, etc. | Online policy forums |

Using the three pillars as a model, problems that occur with the implementation of e-government can easily be overcome. Establishing the right framework for policies and regulatory issues, organizational aspects, and channels and modalities will allow e-governments have a more structured way of operating and handling any of the aforementioned issues.

4. The Role of Information Security in E-government

Information Security and Information Security Systems

In the management and security of all systems primarily raises the question of its kind management - centralized or
regional intellectual kind. Not any centralization system immediately appears many issues and problems. It is on this e – government should be centrally and management, and to ensure the protection and the provision of public services. Centralization and unified technology protection system will ensure the confidentiality of information E – government her safety at all levels of importance and provides great convenience in management.

But above said can be attributed to the technological environment. According to many European, American and Asian government organizations, anti-virus protection of any corporation in the information plays an important role the staff itself. It refers to the staff about 70% of the loss, alteration, loss of reliability of the information, etc. situation in the process. This training to protect sensitive information on the manifest to the consciousness itself is a relevant step. And after that legislative legal protection of information and education of citizens to preserve the confidential government information.

In all countries of the world operates many state or private enterprises that provide services to citizens of different types. For example - for connection to its full web. And government organizations and commercial enterprises providing services for connection to the local network or global course for all different types of protection system. But they not only protect the system and software (software) to connect users to the network of different types. When one speaks of the state system as mentioned above in politics and security architecture of information resources need to clearly specify all requirements for connecting to state information resources. This applies to all telecommunications, television broadcasting and other businesses that provide various types of query or other type of receiving information (eg using personal computers, mobile devices, from different kiosk using ID-card, etc.). And of course the level of the registration, authorization, identification and authentication should correspond to the level of significance of the information. And control of the action should take place around the clock instantly writes intelligently reporting user action.

Information is broken down into many definitions, some of which are syntactic, semantic, and pragmatic. Information security, or InfoSec, according to the generally used definition, is broad. InfoSec involves the protection of various forms of data, services, systems and electronic communications from risk using appropriate measures. The diversity of definitions broad, but most commonly used definitions are as follows:

1. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. 44 U.S.C. § 3542 (b) 91
2. Information security is also characterized as the preservation of:
   a) Confidentiality: ensuring that information is accessible only to those authorized to have access.
   b) Integrity: safeguarding the accuracy and completeness of information and processing methods.
   c) Availability: ensuring that authorized users have access to information and associated assets when required. ISO/IEC 27000 series (17799)
3. A state and a process of information balance which is beneficial for a proprietor of information resources.

Confidentiality, Integrity, and Availability (CIA) according to the second definition is the most comprehensive and relevant when exploring modern information security (InfoSec) issues. Imagine transmitting extremely large quantities of data, for example, how will we maintain the confidentiality of this information and made sure that the intended recipients were the only ones who have access to it. Also, when this data is transmitted, will it arrive as intended and maintain its integrity? Considering availability, what authorization methods for this data will be required and how will it be accessed?

When building an InfoSec system, it is also necessary to consider seven additional principles: Taking into account all possible and interconnecting threats, Continuity, Complexity, Optimization, Flexibility, Simplicity, and Openness. Encompassing all of these principles through a single disciplinary approach is impossible, which is why when building an InfoSec system it is essential to include participants from a variety of disciplines to ensure that the system will truly encompass and incorporate all of these aspects into it. Also, InfoSec is not a single isolated system, but a networked system which requires a certain level of continuity. InfoSec systems should always be developing and evolving, full of renovations when necessary. Nevertheless, constant renovations and changes to the system may also render it vulnerable and possibly ineffective if done too much.

5. Vulnerabilities and Threats

When considering the implementation of an InfoSec system taking into account who will be using the system is essential. There are two basic types of potential users in an InfoSec system: Adversaries and Users.

A personalized system for the users builds a model of the goals, preferences, and knowledge of each individual and uses this model to guide interaction with the user. The system should be adaptive and the users should also have proper preparation before using the system. It is necessary to make users think collaboratively and work together in such a manner.

The personalization and real-time adaptation of not only users, but adversaries as well, should also be taken into account. Adversaries being any potential entities that could access the system with the intent of causing harm in some way, shape, or form. Theoretically, the personalization of a system by collecting information about the users and adversaries and fusing it into a single coherent model would
be ideal. But constructing such a model might be a difficult task, but is feasible for a group of experts in diverse fields who work together.

The National Strategy for Homeland Security in the US categorizes critical infrastructures into the following sectors: Agriculture, Food, Water, Public Health, Emergency Services, Government, Defense Industrial Base, Information and Telecommunications, Energy, Transportation, Banking and Finance, Chemical Industry/ Hazardous Materials, and Postal and Shipping. Accidents and emergencies that pose a threat to critical structures may be caused by natural disasters, technical failures, personnel errors, attacks by adversaries, or a multitude of other things. Diverse techniques should be applied to protect against accidents and emergencies, as well as focusing on recovery in the event that an emergency does occur. Understanding what information is, and the concept behind information security, is essential for developing methods to defend a nation’s critical assets.

The ISO 27000 provides us with suitable guidelines that should be followed if want to be able to identify any vulnerabilities or threats properly. Special terminology, definitions, and issues to be considered according to ISO 27000 are as follows:

1. RISK MANAGEMENT - Risk management is the identification, assessment, and prioritization of risks (defined in ISO 31000 as the effect of uncertainty on objectives, whether positive or negative) followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events[1] or to maximize the realization of opportunities.

2. Implementation and Security Policy
   Principal Questions on InfoSec:
   • Who’s proprietary is the Information Resources and Processes? (Eternal problem of balance, Secrecy and Openness – the result of contradictions between Proprietaries)
   • What are the metrics of InfoSec?

3. Organizational Implementation and Security
   Bringing users into the loop early makes them stakeholders in the policies and ambassadors to the rest of the society.

4. Asset Management - Asset classification and control, accountability and responsibility.

5. Human Resources Security – Who is involved in the process makes a great difference.

If it is another team, no doubt Supercourse will be developed otherwise.

Codes of practice if you follow ISO 27000 also include:
6. Physical and Environmental Security
7. Communications and Operations Management
8. Access Control
9. Information Systems Acquisition, Development, and Maintenance
10. Information Security Incident Management
11. Business Continuity Management
12. Compliance

6. Proposed Solutions

Information security techniques combined with the ideologies of ISO 27000 will help to formulate new policies, clarify new threats, identify barriers, name adversaries and competitors, and to help provide continuity in E-government. Following an open government approach based around transparency, interactivity, and the three pillars will help to set a fundamental guideline for setting open government goals. The three pillars will help to establish policy and regulatory framework, organizational framework, and channels and modalities that will help to deal with the problems identified above.

Furthermore, librarian science and technologies will support the dissemination of information severely, and give it a solid base. The development and use of open source networking tools that are sophisticated and easy to use at the same time will help practitioners to accomplish any goals set and overcome barriers and obstacles. This software should be capable of moving data to a specific data center that will help facilitate sharing across silos.

A legal approach to resolving many of the aforementioned issues would be to first persuade various societies throughout the world that these concepts and ideas are in fact true when it comes to E-government and open government. The next step would require us to overcome any bureaucratic and judicial barriers that may impede the development and implementation of such E-government policies. Last of all, the elaboration of various codes of practice based on information security, ethical, and legal aspects to create a multidisciplinary approach to bridging intercultural barriers.

7. Conclusions

E-government system should first of all ensure the confidentiality of information and information resources state. By organizing security and training of citizens to preserve and allow to minimize the human factor in the protection of information at government level. Second - the security system needs to be centralized. For complete control over the actions and influence the different event. Third - the security policy and security architecture must be built on a single standard to ensure the confidentiality of information in order that the user would have to provide services and the organization of the connection is convenient, fast and easy while preserving the reliability of information.

The issues surrounding the development and implementation of E-government systems are highly complex, but with the right approach can be easily resolved.
Information security issues, legal issues, networking issues, and other various issues that arise from moving toward an E-government can be remedied by following the guidelines that have been established by ISO 27000 and other researchers in the field. The implementation of these ideas can be realized through practice, research, and academic means. It is necessary to implement a strong cross-silo approach in order for things to function in an appropriate and effective manner. A multidisciplinary approach is crucial to solving many of the issues we are faced, and is necessary if we want to implement good E-government systems and promote open government successfully.

REFERENCES

[1] Dr. Shailendra Singh “E-Governance: Information Security Issues”, International Conference on Computer Science and Information Technology (ICCSIT’2011) Pattaya Dec. 2011 pp 120-124;

[2] Rabah Alshboul “Security and Vulnerability in the E-Government Society”, Al Albayt University Department of Computer sciences Contemporary Engineering Sciences, Vol. 5, 2012, no. 5, pp 215 - 226;

[3] T.I. Buldakova, B.V. Glazunov, N.S. Lyapina “Assessment of efficiency of protection of systems of electronic flow of documents”, Mathematical foundation and theoretical aspects of information security, Report TUSUR № 1 (25) part 2 2012 June, pp 52-56;

[4] S.K. Ganiev, M.M. Karimov, K.A. Tashev, “Information security” Tashkent 2013 pp 250-300;