Macrothink Institute™

Journal of Management Research
ISSN 1941-899X
2012, Vol. 4, No. 4

E-Government and Security Requirements for Information Systems and Privacy (Performance Linkage)

Mohammad Hazza Zu'bi
Instructor, Faculty of Planning and Management Systems
Department of Management Information Systems, Al- Balqa' Applied University

Hamdan Hasan AL-Onizat (Corresponding author)
Instructor, Faculty of Planning and Management Systems
Department of Management Information Systems, Al- Balqa' Applied University
E-mail: enizat80@hotmail.com

Received: July 1, 2012 Accepted: September 20, 2012 Published: October 1, 2012

doi:10.5296/jmr.v4i4.2088 URL: http://dx.doi.org/10.5296/jmr.v4i4.2088

Abstract

This paper aims to review the literature related to e-Government and security requirements for information systems and privacy in the performance approach, security is a global problem that requires global and multi-dimensional response with respect to policy, socio-economic, legal and technological aspects. E-Government as a public sector faces a challenge due to its impact on security and privacy. E-Government can develop information security metrics that measure the effectiveness and efficient of their security and privacy to provide information that can be analyzed in the context of e-Government performance to avoid all kinds of threats.

Keywords: E-government, Performance, Privacy, Security, Security policy

1. Introduction

The major aim of this paper is to present a literature review for the e-Government and security requirements for information systems and privacy. With the popularity of computer network technology and sharing of a large amount of government information. E-Government is a kind of governmental administration which based on electronic information technology. The spirit of e-Government is using electronic information technology to break the boundary of administrative organizations, and build up a virtual electronic government. People can get government information and services through electronic media. Governments can communicate with each other through various kinds of electronic media which can be used inside government bodies, between different governments, or between government and society. However, there are many problems exposed in the spread of computer network technology. Security and privacy are the most important aspects related to the E-Government performance.

2. Background

Electronic government (e-Government) is no longer just an option but a necessity for countries aiming for better governance (Al-Onizat,2011). In recent years there has been a great proliferation of e-Government. E-Government is a general concept in the world referring to the government's effective use of modern information and communication technologies, through various information services, e-Government as a virtual organization to provide public management and public service, not normally engaged in the creation of material resources (Isaac,2007). E government is narrowly defined as the use of information technology, especially the Internet, to deliver government services and information to citizens, businesses, and other government bodies (Holden, Norris, & Fletcher, 2003). Office of Management and Budget (2002) identifies four key categories of customer groups that interact with government agencies and provide opportunities to transform delivery of e Government services. They are:

• Government to Citizen (G2C): Individuals accessing services or information

• Government to Business (G2B): Organizations accessing services or information

• Government to Government (G2G): Partner government agencies accessing services or information or integrating services across agency organizational boundaries through technologies.

Isaac(2007) introduces the relationship between the e-Government stockholders,(Figure 1).

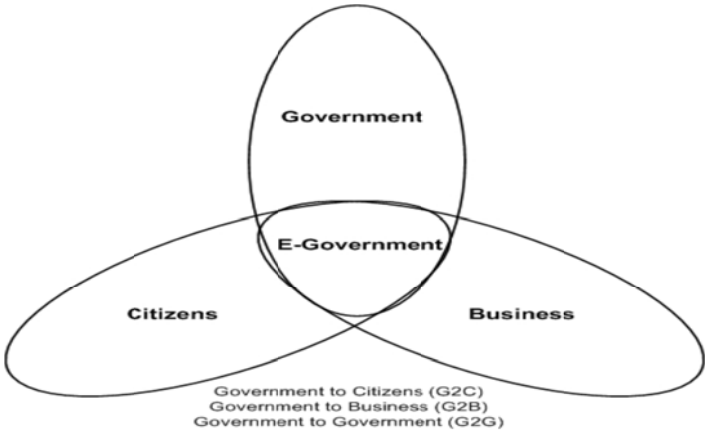

Figure 1. Relationship between major e-Government stakeholders (Isaac, 2007)

Internal efficiency and effectiveness make better use of modern technology to reduce cost and improve quality of government agency administration, by using industry's best practices. There are different performance measurement models to measure the e-Government performance and different studies differ in identifying the key factors and measurement indicator. Al-Onizat(2011) indicate that all of performance measurement models insure that security as critical issue that must be accountable. Security and privacy is important because it affect the performance of the E-government.

3. Information Security Policy

Security measures main aim is to identify all possible threats and vulnerabilities; An information security policy is a plan identifying the organizations fundamental assets with a detailed clarification of what is acceptable, unacceptable and logical behavior from the stockholders in order to effectively ensure information security (Hone & Eloff, 2002). This plan must alignments with the performance level that the e-Government. This performance level must be evaluated to insure the successes with respect to the security measures.

4. Information Privacy

According to Morison (1973), information privacy definitions can develop based in either individual belief or system perspectives (i.e. morals, religious-based, philosophic perspectives, and others). Information privacy definitions also include perspectives that reflect actionable processes that can affect personal privacy, such as protection, use, management, storage, dissemination, and disposal of records or documents that contain personal data (Clarke, 2000; Morison, 1973). Examples include the U.S. government and commercial interest's perspectives where individuals are primarily responsible for use of personal data and should take active interests and responsibility in managing personal data. (Morison, 1973). All stakeholders in the context of e-Government will be reluctant to use the web based services offered by the e-Government, due to their poor skill, lack of confidence, security and privacy concerns, which will affect the e-Government performance.

5. Security in E-government

Security is one of the most important issues in E-government. A crucial part of managing information security is having a framework and set of standards to which all the necessary areas of information security in the organization adhere (Tassabehji& Elliman,2006). Many studies have revealed that there is a link between security and e-Government (Siponen and Oinas-Kukkonen, 2007). The security dimension is the ability of the site to provide secure access to all applications and facilities provided by the e-Government (Tojib et al., 2006). The data and information being manipulated within e-Government processes may be more sensitive than those in e-commerce processes (Wimmer & Bredow, 2002). Public(government) private partnerships will be promoted wherever feasible to enlarge the resource pool without compromising the security aspects and for this purpose. Trust is a crucial aspect in the e-Government to achieve a high level of performance when the outcomes measurement applied.

6. Information Security Threats in E-government:

A threat is simply any event that, if realized, can cause damage to a system, and create a loss of confidentiality, availability, or integrity (Coelho, 2007). Mazumdar (2009) point the most important threats that can be face the E-government, and it can affect the performance of the e-Government.

6.1 Client End Threats

Until the introduction of executable Web content, Web pages were mainly static. Coded in HTML, static pages could do little more than display content and provide links to related pages with additional information. But, the widespread use of active content has changed this perception.

6.2 Communication Channel Threats

The Internet serves as the electronic chain linking a consumer (client) to the e-governance server. Messages on the Internet travel a random path from a source node to a destination node. It is impossible to guarantee that every computer on the Internet through which messages pass is safe, secure, and non-hostile.

6.3 Server end Threats

The server is the third link in the client-Internet-server trio embodying the e-Governance path between the citizen and the government. Servers have vulnerabilities that can be exploited by anyone determined to cause destruction or to illegally acquire information (Mazumdar, 2009). All those threats according its nature can make a problems for the both citizen and the e-Government.

There are many security aspects according the e-Government models, This aspects include: Integrity, Availability, Data validation, Sensitive data, Authentication, and Confidentiality. Nath (2005) classify those models as the following: Broadcasting / Wider-Dissemination Model, Critical Flow Model, Comparative Analysis Model, E-Advocacy/ Lobbying and Pressure Group Model, and Interactive- Service Model. Threats differ according to data locations: data in store, data in process, data in transit and data in destination. E-Government

has a responsibility to provide leadership in developing a culture of privacy protection and security. It should provide this leadership through its roles in the development of public policy, as owner and operator of systems and networks, and as a user of such systems and networks. As a user of information systems and networks, government shares a role with businesses, other organizations and individuals for ensuring secure use of the system and network.

7. E-Government Performance and Security

Performance measures should be indicated directly (Al-Onizat,2011), from the organization's mission statement, strategic issues, goals, and objectives (Stowers,2004).West (2000) used an evaluation approach for the E-Government developed only on the basis of characteristics found by observing Web sites (e.g. phone contact information, addresses, publications, databases, foreign language access, privacy policies, security policies, an index, disability access, services, email contact information, and search capabilities, etc). This approach explains how the security and the privacy aspect affect the performance level. Most the existing performance measurement are quantitative (e.g., number of websites, decrease in response time to questions, etc.), But few include qualitative measures related to policy and ethics, whether privacy policies are included on websites or local government officials the aware of privacy protection must be measured. (Henriksson et al., 2006) divided the factors that influence the quality of government websites to 6 major categories: (1) Security and Privacy; (2) Usability; (3) Content; (4) Services; (5) Citizen Participation; and (6) Features. Although some efforts are being made to develop metrics, no systematic set of quantitative and qualitative measures have been developed for widespread use (Carbo & Williams, 2004). Alazazi (2008) developed a model for e-Government information security evaluation, compose of five layers. Each layer represents a dimension of security which needs to be addressed in order to mitigate threats associated with it. It has one or more of sub layers. The number of sub layers will be determined by number of security measures an e-Government organization feel sufficient to provide an acceptable security level. The only model reflects the layers and sub layers required to provide an acceptable security program for any e-Government organization offering services to the public citizens. The model establishes, the sub layers is the most required for the security program to tackle the multiple threats associated with an e-service. This linkage between security and performance insure the relationship between them. Along with security are issues of privacy of information and trust of users or citizens which is a superset of security (Patton & Josang 2004) also identified in e-commerce literature as a main obstacle in the growth and adoption of e-commerce. Alazazi compare between Security models and standards. Figure (2) show the comparison.

Characteristics	Models and Standards								
	Non Deducibility	Non Interference	Bell Lapadula	Bba	Chinese wall	BS7799	BSI IT	COBIT	multi-layer
Structured in Layers	x	x	x	x	x	x	x	x	√
Coverage of Sec Aspects									
Technology	x	x	x	x	x	x	x	x	√
Policy	√	√	√	√	√	√	√	√	
Human behavior and awareness	x	x	x	x	x	x	x	x	√
Ops and Mgmt	x	x	x	x	x	√	√	√	√
Explicitly explained	√	√	√	√	√	√	√	√	√
Government or commercially	√	√	√	√	√	√	√	√	√
Applicability to any sector	√	√	√	√	√	√	√	√	√
Within One System or entity	√	√	√	√	√	x	x	x	√
Within Several Systems	x	x	x	x	x	√	√	√	√

Figure 2. Comparison between Security models and standards:(Alazazi, 2008)

characteristics	Models and Standards								
Structured in layers	×								
Coverage of Sec Aspects									
Technology	√								
Policy									
Human behavior and awareness									
Ope and Mgmt									

explicitly explained									
Government or Commercially									
applicability to any sector									
within one system or entity									
within several systems									

Performance measures are a key feedback mechanism for an effective information security program in e-Government can develop information security metrics that measure the effectiveness of their security and provide data to be analyzed. The United Nations insure the principles for successful e-Government according to security and privacy concerns, it must be addressed early on, openly and with demonstrated professional ability (United Nations, 2003).

8. Conclusion

This paper has examined the issue of e-Government from the perspective of security and privacy. The leadership of the E-Government must establishing the information security programs, setting program goals and priorities that support the mission of the organization, and making sure resources are available to support the information security program and make it successful. The investment in the in information security must be developed, focus on critical information security goals; determine the key activities to build an effective information security. Performance measures are a key feedback mechanism for an effective information security in the E-government. The leadership of the e-Government can develop information security metrics that measure the effectiveness and efficient of their security and privacy to provide data that can be analyzed in the context of e-Government performance to avoid all kinds of threats.

References

Al-Azazi, S. (2008). A multi-layer model for e-Government information security assessment, Ph.D. thesis, Cranfield University.

Al Nagi, E., & M. Hamdan. (2009).Computerization and e-Government implementation in Jordan: Challenges, obstacles and successes. *Government Information Quarterly, 26*, 577-583. http://dx.doi.org/10.1016/j.giq.2009.04.003

Al-Onizat H. Hamdan. (2011). A Web based Model for Evaluating E- Government Performance (Jordan), Unpublished Dissertation, Jinan University.

Carbo, T., & Williams, J. G. (2004). Models and Metrics for Evaluating Local Electronic Government Systems and Services. *Electronic Journal of E-Government, 2*(3).

Clarke, R. (2000). Beyond the OECD guidelines: Privacy protection for the 21st century. Retrieved March 13, 2008, from: http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html.

Coelho. (2007). Security Certification For Organizations A Framework To Manage Information Security, Stituto Superior de Ciências do Trabalho e da Empresa.

Henriksson, A. Yi, Y. Frost, B., & Middleton, M. (2006). Evaluation instrument for e-Government websites, Proceedings Internet Research 7.0: Internet Convergences, Brisbane, Queensland, Australia.

High Level Seminar On Measuring And Evaluating E-Government And Back-To-Back 3rd Meeting Of The Working Group 2 On E-Government And Administrative Simplification. (2007). Measuring and Evaluating E-Government in Arab Countries.Dubai School of Government

Holden, S. H., Norris, D. F., & Fletcher, P. D. (2003). Electronic government at the local level: Progress to date and future issues. *Public Performance & Management Review, 26*(4).

http://dx.doi.org/10.1177/1530957603026004002

Institute for development Policy and Management. (2008). What is e-Government?. Accessed on 4th December 2010: http://www.egov4dev.org/success/definitions.shtml#definition.

Mazumdar, Chandan, Kaushik, Anil K., & Banerjee, Parthasarathi. (2009). On Information Security Issues in EGovernance: Developing Country Views. *CSDMS journal,* 6th July.

Morison W.L. (1973). Report on the Law of Privacy. Sydney, Australia: Government Printer.

Patton, M., & Josang, A. (2004). Technologies For Trust In E-Commerce. *Electronic Commerce research, 4*(1&2), 9-22. http://dx.doi.org/10.1023/B:ELEC.0000009279.89570.27

Stowers, G. N. L. (2004). Measuring the Performance of E-Government. Accessed on December, 3, 2010, from:http://www.businessofgovernment.org/pdfs/8493_Stowers_Report.pdf

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *SIGMIS Database, 38*(1), 60-80. http://dx.doi.org/10.1145/1216218.1216224

Tassabehji Rana, & Tony Elliman. (2006). *European and Mediterranean Conference on Information Systems (EMCIS)*.Spain. http://dx.doi.org/10.1504/IJASM.2006.011628

The Performance Institute. (2002). Creating a performance-based electronic government. Accessed 2end December 2010: http://www.cio.gov/archive/egovernmentreport.pdf

Tojib, D. R., Sugianto, L., & Sendjaya, S. (2006). A conceptual model for B2E portal user satisfaction. Proceedings of the International Conference on Business and Administration (BAI), Singapore.

United Nations. (2010). United Nations E-Government Survey. Accessed on December, 22. from: http://www2.unpan.org/egovkb/global_reports/10report.htm

West, D. (2000). Assessing E-Government: The Internet, Democracy, and Service Delivery by State and Federal Governments, Brown University, September. Available: http://www.brown.edu/Departments/Taubman_Center/polreports/egotreport00.html .

Willy C. Isaac. (2007). Performance Measurement for the e-Government Initiatives:A Comparative Study. ProQuest Information and Learning Company. 300 North Zeeb Road.

Wimmer, M., & Bredow, B. V. (2002). A holistic approach for providing security solutions in e-government. *Proceedings of the 35th Hawaii International Conference on System Sciences (HICSS 35 02), 5*, 1715- 1724. http://dx.doi.org/10.1109/HICSS.2002.994083