Class Project Book Chapter Innovations in Information System Series: 3 | Year: 2017 | ISBN: 978-967-0194-97-4

### 5

### E-GOVERNMENT SERVICE SECURITY

Jama Mohamed Jama, Othman Ibrahim

#### 5.1 INTRODUCTION

E-government service security approach is one of the most important elements as a part of government policy. The aim of this is for designing protection mechanisms for government transactions over the information communication technology. For several decades governments has increased their level of protection in order to improve their functions' efficiency and effectiveness. As such, to promote government's defense systems from future internal and external threats, security becomes a key demand and vital to be implemented. This book chapter reviews the current egovernment service security and the methodology used to study existing implementation of e-government service security.

#### 5.2 E-GOVERNMENT CONCEPT

The concept of an e-government system is to provide access to government services anywhere at any time over open networks. This leads to issues of security and privacy in the management of the information systems. Managing such issues in the public sector has different emphases than in the private sector of the entity. The broader e-government approach is socio-technical by nature, involving people and processes as well as technologies; hence, particularly in transitional countries, the social culture and characteristics of the country are factors in successful e-government development. In the open literature there are four distinct aspects to e-government. The following section gives an overview of this literature.

#### 5.3 E-GOVERNMENT SECURITY

Public and private organizations are facing a wide range of information threats. With these threats, e-government requires guidelines for effective information security management practices.

E-government became increasingly dependent on technology and internet to support online systems' activities. For e-government, security plays an important role to protect data from an authorized user, accidental loss, destructions, disclosure, modifications, misuses or access to confidential information. Moreover, with increasing reliance on technologies connected over open data networks, effective management of information security has become one of the most crucial success factors for both public and private organizations. In certain cases there are also many security failures due to human factors [8]. As such, best practice of security management is required and this takes a holistic organizational approach which incorporates an organization's business processes, controls and policies; corporate governance; human resource management and training; and organizational technology culture as well as systems and infrastructures [6, 7]. Along with security are issues of privacy of information and trust of users or citizens which is a superset of security [5] also identified in e-commerce literature as a main obstacle in the growth and adoption of e-commerce ([6, 9])

#### 5.4 CHALLENGS OF E-GOVERNMENT

There can be different challenges in the success deployment of egovernment in any country. The following are the major issues while considering about e government [1, 2, 3, 4].

(a) Access Issues: This provides direct access to the information, in which some of this information requires to be converted to a

digital form. All e-government information system must have mechanism to protect citizens' security and privacy. This is the way to measure that a complete privacy policy has been installed another way to measure security and privacy is by keeping the information of e-government website.

- (b) **Technical issue:** Integration of old computer systems to a new internet based platform is time consuming and costly. It requires technical experts. Changing new technology and maintenance in this part requires consistent update on current technology trend. A website must be embedded with the last application and features and the content and information of the website must be up to date.
- (c) **Human factors:** Transforming cultural behavior is difficult due to fear of the new technologies, worry of job loss etc. Certain techniques and methods are required to measure citizen satisfactions. This is to ensure that the e-government applications implemented is functioning. Citizens need encouragement reassurance of their job prospect.
- (d) **Service Delivery Issues:** Issues in financial transaction whereby many people are aware of the risk in providing credit cards information via the Internet. Therefore adequate protection of e-government transaction is necessary to obtain the trust of e-government customers.
- (e) **Delivery Integrated Services**: Individual state agencies are not convinced with the value of integrated services. All this while, dealings are done on local basis and these state agencies are comfortable with this operational manner. This is the reason why they are not willing to involve with technologies that facilitate integrated services.
- (f) **Resource issues:** Human resource availability is part of any egovernment implementation. Staff should get adequate training and knowledge to use the technology for e-government

applications or services. The reason is new technologies are more complex and e-government applications are more equipped.

(g) **Other Issue:** Government officials are concern on suggestion of e-government, and government often makes important changes to the organization. Changes to licenses and permits seem to be increasingly occurring in the country or State government. These changes require technology update.

With these changes, government officials are concern with the need to reduce the staff job reformation.

#### 5.5 IMPORTANT OF E-GOVERNMENT SECURITY

E-government service faces a lot of security problems. To protect citizen's privacy and security, these problems are identified below [6].

- (a) **Information Intercepting:** Information intercepting is process of stealing information from users or any other. Hackers can do this kind of intercepting to make fraud to e-government systems.
- (b) **Information Tampering:** Information tempering regards to the internet interfere; these involve adding, modifying or erasing original dates and damaging essential data. Malicious users can find or navigate the database to retrieve and modify contents.
- (c) **Services Denying:** Denial of service is a method of trying to make the computer resource busy so that hackers will send more data packet to the system to get stack and jam the server. This will make the computer stops and the services will be unavailable. It is mainly comes from the attacker or viruses or artificial destruction of the devices.
- (d) **Information Faking:** Attackers could make up as authorized user or build false information to deceive other users. This is normally

done after they recognize the regulations of the network information or they had decoded the sensitive information. Attackers mostly pretend as users to get unlawful certifications, making faking emails, etc.

#### 5.6 METHOD OF RISK ANALYSIS IN E-GOVERNMENT

Risk analysis is refers as a method of identifying risks, analyzing risks, and making up risk managing plans. In e-government, the measures of security risk are; risk identifying, risk analyzing, and risk controlling.

#### 5.6.1 Risk Identifying

Risk identifying is the first step in risk management so that security risk of e-government can be adopted. As such it is necessary to detect and gather risk from different significant threats, risk problems and their related countermeasure. In addition, it is also necessary to acknowledge some feasible risk and threat of electronic government system.

#### 5.6.2 Risk Analyzing

Risk analysis is the step to determine the importance of all components in e-government and categorizing factors that could bring threats and risk. These factors need to be assessed and analyzed to determine which are more vulnerable to cause risk. Therefore, it is important to understand the source of the risk, which could be from the environments, people, and nature and so on. Table 5.1 shows the possible threat sources. Several ways can be used to recognize threats. Examples are brainwashing in Delphi and scenario analysis.

Threats	Possible Sources
Intentional Threats	Terrorist
	Criminals
	Hackers
	Cyber internet attack
	Viruses
	Fraud
	Theft of resources
	Denial of service
Unintentional Threats.	Mis operational from system users
	Mis-operational from system
	Administrators and protectors.
Natural Threats	Earth Quick,
	Electricity shock
	Floods
	Thunder and lighting

Table 5.1         Possible Threat Source
--

#### 5.6.3 Risk Controlling

Risk controlling the step to verify whether the risk analysis has been achieved or not. The objective of e-government security risk control is to reduce risk level and measure any electronic government projects which are currently suffering. There are two broad methods of risk controlling. The first is risk controlling measure, such as risk falling, avoiding, or transmitting and losses managing. Second are measures to support risk reimbursement in terms of financial.

#### 5.7 GOVERNMENT SECURITY MODEL

Security of e-government systems has to be managed systematical, and continuously [3]. It has to be created with necessary level of confidence and trust among the stake holder, citizens, business, and government. It must be also stander of security practices and implement in e-government. The e-government security model is mainly consists of three different areas and each of them is subjected to various types of threats. In addition, for each Area requires security measures: The *User's Environment, Transport Environment and ICT Assets Environment.* Figure 5.1 give examples of e-government security model.



Figure 5.1 Model of E-government Security

#### 5.8 METHODOLOGY

The respondent of this study was a group of technical staff from Nusajaya ICT department in Johor Bahru. They have basic background of e-government service and security implementation methods. Preliminary survey was conducted to choose the target respondents in which the survey will focus on. The most important target was to know and identify the current situation Priority was also placed on the respondents in the sense that, the respondent must be a staff member of Nusajaya ICT centre. Data obtained from the survey was analyzed using SPSS. The descriptive procedures in SPSS provide mean value and Standard Deviations (SD) for variables. It also provides the minimum and maximum value. It is a good practice in Likert Scale questions to print means for since the number that is obtained can provide an indication of what average answer is. The SD is also important because it gives us an indication of the average distance from the mean. The low SD means the most observations center around the mean. Conversely, the high SD means that there were a lot of variations in the answers. SD of 0 is obtained when all responses to a question give the same answer.

#### 5.9 FINDINGS OF THE STUDY

The demographic variable that was used in this research was gender, so Table 5.2 below gives the respondents' profile gender

Gender	No. of respondents	Percent
Male	24	40
Female	36	60
Total	60	100

Table 5.2Profile Gender

The figure above shows the details of survey respondents by gender. There are more males in comparison of female, out of 21 respondents who gives their feedback 60% were Males while 40% are female.

#### 5.9.1 Identifying Risks on E-Government Service

1 able 5.5	Risk on E-Government Service Denvery						
E-government risks	Number of	Min	Max	Mean	SD		
	Respondent						
Hacking	21	1	5	3.33	1.065		
Cyber Attack	21	2	5	3.48	.981		
Internet Worm	21	1	5	3.05	.921		
Attack							
Denial of service	21	2	5	3.38	1.024		
Viruses	21	2	5	4.19	.928		

 Table 5.3 Risk on E-Government Service Delivery

Table 5.3 shows great varies among e-government risk. Five risks were examined in this survey. To present the outcome of the

survey, mean and Standard Deviation was used. Five-point scale is used whereas 1=Not important, 2=less important, 3=neutral, 4= important, and 5= most important. As it shown in Table 3, viruses have a higher mean value which is 4.19. There is also a significant increase in Cyber attack, Denial of service. Conversely, internet worm attacks (3.33) have lower ratings. Based on this important statistics, it can be concluded that viruses, cyber attack and Denial of service are the highest risk on e-government services delivery and should be considered seriously as risk in e-government. Similarly, internet of worms and hacking could be another source of threats but have lower rate.

## 5.9.2 Applying the Most Appropriate Security Components in E-Government Service

Contents	No of	Min	Max	Mean	SD
	Respondent				
Password	21	1	5	4.29	1.146
Digital Identity	21	1	5	3.86	1.153
Biometric device	21	2	5	3.81	.928
Access Control	21	1	5	3.71	1.189
E-government	21	1	5	3.76	1.261
Gateway					

**Table 5.4** Security Components Appropriate to E-government Services

Table 5.4 shows the respondent's perception on security management tools appropriate in e-government service. All respondents answered positive to the security tools applicable in e-government service. As observed on the table, the mean value on password is 4.29 along with Digital Identity 3.88 and Biometric device 3.81. Respondent also indicated that there is increase on e-government gateways 3.76 and access control 3.71 respectively.

#### 5.9.3 Applying the Most Appropriate Security Technology

Contents	No of Respondent	Min	Max	Mean	SD
Data Backup System	21	2	5	4.33	.966
Encryption Methods	21	2	5	3.90	.995
User Security ID	21	2	5	4.19	.981
Management					
Internet Security	21	3	5	4.33	.856
IDS/ and other detection	21	1	5	3.57	1.165

 Table 5.5
 Security Technologies in E-government

Table 5.5 shows 5 types of technologies that organization uses as security purpose. Based on the table's contents majority of the respondents believe that Data backup system 4.33, internet security 4.33 and User Security ID 4.19 are most widely used security technology in e-government. The least technology for security is the one who obtained the lowest mean value. The result is encryption 3.90 and IDS 3.57

## **5.9.4** Applying the Most Appropriate Security Technology and Activities.

Contents	No of Respondent	Min	Max	Mean	SD
Network firewall	21	2	5	3.95	.921
Network Intrusion Detector	21	2	5	4.00	1.000
Network Access Control	21	2	5	3.76	.944
Server & work station security	21	2	5	4.05	.865
Anti viruses	21	2	5	4.10	.944

 Table 5.6
 Security Components and Activities

Table 5.6 shows network security components and their role of security in e-government service. Most of the respondents strongly believe that Ant viruses 4.10, Server Work station security, Network Intrusion detector 4.0 3.05 are the most reliable network security components which plays a vital role of monitoring traffics and prevent an authorized access. It also shows that there is a low decrease in the mean value for Network firewall, which is 3.95 and Network access, which is 3.76 respectively.

# 5.10 PROPOSED MODEL OF EGOVERNMENT SERVICE SECURITY

The global IT revolution is growing rapid and governments are ready to provide their secure online service to their citizen using ICT. However trust on e-government transaction, to promote communication and interactions, government bodies and their managers must fully implement privacy and security to the egovernment services. The author of this research proposes full detailed e-government security model which is mainly consist of 4 parts. 1) e-government Users, 2) process required users 3) ICT and Security Components, 4) e-government service as shown in the Figure below. This model was developed by adapting the mode of E-Government Security.



Figure 5.2 Refined E-government Security Model

#### 5.11 BOOK CHAPTER SUMMARY

This book chapter contains discussion on e-government security process including risk security aspects. It also explains importance of security and roles that security plays in e-government, challenges of e-government, methods for risk analysis and risk factors of egovernments. This study has discussed the methodology for identifying risk factors as well as the major challenges that arise in information communication technology. It also discussed the proposed model of e-government Service Security in Malaysia, for better achieving Citizens privacy, security and trust on e-government services.

#### REFERENCES

- [1] Gelbsein, E. (2001). 'Managing Information Security'. OECD Workshop, International Computing Centre, Geneva. http://accsubs.unsystem.org/ccaqfbintranet/Accessed 20/2/2004.
- [2] Higgins, H. N. 1999. "Corporate system security: towards an integrated management approach." Information Management and Computer Security ,7(5): 217-222.
- [3] J.Satyanarayana, (2004) E-government: The science of the Possible. New Delhi, Prentice-Hall Private
- [4] Lauren May, 2009 Information institute of Security School of Management Queensland University of technology, Brisbane, Australia
- [5] Patton, M.A., & Josang, A. (2004) "Technologies for Trust in Electronic Commerce" Electronic Commerce Research",4:9-21
- [6] Tassabehji (2003) Inclusion in e-government Security perspective: University of Bradford in Uk
- [7] Tassabehji (2005) Principles for Managing Information Security'.Encyclopedia of Multimedia Technology and Networking, Pagani, M. Ed.pp.842-848. Idea Group Reference
- [8] Weirich, D. and M. A. Sasse 2002. Pretty Good Persuasion: A first step towards effective password security in the real world. ACM/SIGSAC New Security Paradigms Workshop, New Mexico.
- [9] Yousafzai,S., Pallister, J.G., Foxall, G.R., 2005. 'Strategies for Building and Communicating Trust in Electronic Banking: A Field Experiment'. Psychology & Marketing, 22(2):181-202