E-government Security Management: Key Factors and Countermeasure

WANG Jin-fu
School of Management, Xi’an Polytechnic University, Xi’an, P.R.China 710048
jinfubest@163.com

Abstract—Almost all of United Nations member countries now operating government web sites—called e-government. Its implementation is based on information technology which is now as important as tanks, ships, and aircraft in any nation’s defense. So nowadays, with the fast development of information technology, e-government security is considered one of the crucial factors for achieving an advanced stage of e-government. As the number of e-government services introduced to the user increases, a higher level of e-government security is required. This article aims to formulate the key factors for security management. Firstly introduce the concept of e-government and information security, presents a review of ICT management in the public sector, information security management and e-government in recent literature by focusing on issues and trends. The paper then for successful e-government security management analysis the key factors. Put forward a managerial conceptual framework followed. Finally, the corresponding countermeasures for e-government management are proposed.

Keywords- e-government; Security; information system

I. INTRODUCTION

The essence of e-government is using electronic information technology to break the boundary of administrative organizations, and build up a virtual electronic government. Provision of electronic government services is one of the main goals of many governments in the digital world. Public and private organizations are facing a wide range of information threats. Information security is a crucial component in their information systems. With their increasing reliance on technologies connected over open data networks, effective management of information security has become one of the most crucial success factors for public and private organizations alike. It was said by National Computer Network Emergency Response Technical Team/Coordination Center of China (CERT) in 2007, they had received 26476 network security incident reports. This is three times more than 2005 which was reported 9122 network security incidents. As a result, with the fast development of e-government; it is particularly important to strengthen security consciousness and take strong preventive measures in technology and management aspects.

Studies have shown that there is a link between security issues, e-government and management (Siponen and Oinas-Kukkonen, 2007)[1]. Studies have also shown that non-technical issues are as important as technical issues in safeguarding an organization’s sensitive information (Dhillon and Torkzadeh, 2006; Siponen and Oinas-Kukkonen, 2007)[2]. The importance of non-technical issues related to security management, however, is de-emphasized in many studies which tend to be quantitative by nature (Siponen and Oinas-Kukkonen, 2007)[1]. Particularly, with respect to developing countries, there is a resulting lack of attention in the open literature on factors such as the national and organizational culture, environment and level of awareness and how these factors relate to generic attitudes towards information security and its management.

II. LITERATURE REVIEW

A. E-government

The concept of an e-government system is to provide access to government services anywhere at anytime over open networks. This leads to issues of security and privacy in the management of the information systems. In the open literature there are four distinct aspects to e-government: government agencies to government agencies; government agencies to and from citizens; government agencies to and from business organizations; government agencies to and from international organizations and other countries. The remainder of this section gives an overview of this literature. Willingness of citizens and other parties to use e-government services will depend on the trust that they have on the services. E-government services can be public or classified. There are four categories of e-government information and services e-management, e-service, e-commerce and e-Decision making / e-democracy. The challenges in e-government services’ security include identifying users, authenticating users, storing public and classified information in same websites, checking authorities, auditing, signing transactions, resolving conflicts, keeping copies of information, and so on. Hence e-government security systems should be able to meet the following requirements: should provide multiple authentication methods, authorization, credential issuance and revocation, audit, confidentiality, conflict resolution, accountability, availability, platform independent, privacy, information integrity, anonymity, scalability, single sign on and so on.

B. E-government Systems

E-government can be defined as government use of information technologies in order to communicate externally
in the public sector (with citizens and businesses) and internally (with other government departments) (Ebrahim and Irani, 2005)[3]. Accenture (2001) and Ebrahim (2005) give measures for the level of e-government development.

Articles on e-government in some leading countries have been published (Norris and Moon, 2005; Pina et al., 2005)[4-5]. A relationship model of e-government integration has been proposed arguing that the development of effective relationships between central government, individual government agencies and users of e-government services are critical to successful e-government integration. Those barriers show that both technical and non-technical issues should be considered when implementing e-government integration.

A barrier frequently cited is the need to ensure adequate security and privacy in e-government (Conklin, 2007)[6]. Because of the specifics of process in public administration, security models and process models have to correlate. Ebrahim and Irani (2005) and Wimmer and Bredow (2001) have all published articles concerning security and privacy issues in e-government. It is noted that, in fact, e-government itself has become a major contributor to these issues due to its basic concepts of openness and availability.

C. Information Security

Security threats and protective measures for these paper based systems were identified and resolved. They were written into policies and procedures, and updated over many years. This provided a degree of security for documents completely different to that of Intranet or Internet based systems which have the capability to immediately download information, giving the client (end user) the ability to copy and re-transmit this information in nanoseconds. This vulnerability exists for any organization, whether private or public, that has a web presence (Backhouse et al., 2001).

Information system security has previously concentrated on confidentiality of documents stored electronically. In terms of the public perception of government organizations, security means the protection of records and data that are held for the purpose of recording, administering and monitoring the actions and policies of government agencies. This applies equally to paper documents and the data held on computer databases (Kiel, 2003). The rapid growth in the volume of information stored electronically and the uptake of e-commerce within government has heightened the need for increased security to protect the privacy of this information and prevent fraudulent activities (Bradford, 1999).

D. Information Systems Management

Security is traditionally concerned with information properties of confidentiality, integrity and availability. These properties underpin services such as user authentication, authorization, accountability and reliability. Much has been published on the changing role of information security (Dhillon and Torkzadeh, 2006) as its general perception has transformed from the purely technical in the 1970s to its current mainstream role in organizations.

In the broader sense information security involves people as well as technologies. A small number of publications in the literature address the social acceptance of security technologies, known as the organizational security culture (May and Lane, 2006; Siponen and Oinas-Kukkonen, 2007)[7]. Information security standards are well represented in the open literature (Saint-Germain, 2005)[8]. These standards attempt to describe the various processes and controls needed for successfully implementing an information security policy, rather than advising what the policy should look like (Hone and Eloff, 2002)[9]. In general these standards have been developed through the experiences of leading technological countries.

III. E-government Security System Management: Key Factors

A. Architecture of the System

The system contains the following components: an e-government website, an integrated security system, a SAML server, a controller, an e-government client, an e-citizen system, an e-regional system and ministries’ systems.

The functions of the web site include directing e-government clients to different services, policy enforcements, protecting messages, informing the SAML server the required authentication and authorization types before accessing resources and before transactions, backup operations and other administrative procedures. The integrated security system manages digital certificates, smart cards, attribute certificates, registrations and policies. The ISS acts as an assertions’ authority. The SAML server manages authentication assertions, attribute assertions and authorization decision assertions. The controller performs anonymity services. Anonymity can be provided when performing services like electronic voting, survey, e-democracy issues and other issues. The controller performs operations like identifying and authenticating an e-government client. After user identification and authentication the controller removes the original IP address and then sends the message to the desired destination servers with controller’s IP address as source. Another function of the controller is to check the validity of requests. The controller collects credentials of clients. For every serious request there is a denial of service cookie that is a function of an IP address and a secret of a client. This reduces non-availability (partially) problem of the e-government website.

E-citizen system offers a variety of public and classified e-government services to citizens. Public services require no authentication while classified services can require simple or strong authentication with or without authorization. All transactions are protected using the configured security mechanisms. There is a policy file that specifies the types of authentication and authorization needed for each service. If a client desires to perform e-government services at a specific ministry she will be directed to that ministry. Every ministry has a number of integrated security systems and SAML servers at different sections depending on the size of the ministry. Every ministry has its own policies basing on the sensitivity of the information and services it offers. E-regional is a system that deals with local e-government services. The regions or states are in turn divided into
districts. All these regions and districts can have ISS and SAML systems to facilitate effectiveness in the management of services in local governments.

B. Key Factors for E-government System Management

In order to identify the key factors of information security in the public contexts, a conceptual framework that helps us to categorize such factors and understand their environment is needed. The literature on the four aspects (e-government, information security management, IT management in the public sector, and the country context) has suggested several factors that may influence the success of e-government security management. Based on the Ives et al. (1980) model we have identified four major components that are widely believed in the open literature to have the potential to significantly impact on the protection of organizations’ information assets. The four components are: security culture, managerial, information security infrastructures and change management.

<table>
<thead>
<tr>
<th>Key Drivers For Successful IS Security</th>
<th>Average Rank</th>
<th>Ranked Importance Rating</th>
<th>Average Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active support of senior management</td>
<td>1</td>
<td>1</td>
<td>5.5</td>
</tr>
<tr>
<td>Commitment of funding</td>
<td>2</td>
<td>2</td>
<td>5.3</td>
</tr>
<tr>
<td>Protection of information assets</td>
<td>3</td>
<td>3</td>
<td>5.7</td>
</tr>
<tr>
<td>Statutory / legislative requirements</td>
<td>4</td>
<td>7</td>
<td>4.6</td>
</tr>
<tr>
<td>Staff awareness &amp; training</td>
<td>5</td>
<td>5</td>
<td>4.6</td>
</tr>
<tr>
<td>Maintain integrity of electronic records</td>
<td>6</td>
<td>4</td>
<td>4.7</td>
</tr>
<tr>
<td>Negative experience(s) can drive change</td>
<td>7</td>
<td>11</td>
<td>4.0</td>
</tr>
<tr>
<td>Compliance with standards</td>
<td>8</td>
<td>8</td>
<td>4.3</td>
</tr>
</tbody>
</table>

We have chosen the Ives et al (1980) model to appropriately identify the differentiators and requirements needed to be considered by nations for effectively maintaining their information security systems. There are several models of information security in the literature that are based on the concept of the socio-technical approach. The Security By Consensus (SBC) model has been suggested by Kowalski (1994). Dhillon (2000) discusses how socio-technical system approaches can be combined with usability engineering in the design of information systems. Eloff and Eloff (2003) argue that an information security management system (ISMS) consists of many aspects such as policies, standards, guidelines, codes of practice, technology, human issues, legal and ethical issues. The Ives et al (1980) model of information systems (IS) research is widely known and discussed in the information system management literature. The model distinguishes between three information system environments (user, IS development, and IS operations environments) and three information system processes (use, development, and operations processes). The environments component defines the resources and constraints that dictate the scope and form of information systems and IS processes. According to the related works, we identified key drivers for IS Security(table 1). These are the major factors which should contribute to successful IS Security processes within government agencies (Baird et al, 2002).

The issues transcribed are an accurate summary of the related papers. All issues were rated above 4.3 (> moderately important) indicating that all of these issues are worth considering by management as factors that drive successful ISS processes within e-government. In order to differentiate between issues, ranking was carried out which revealed the three major issues (refer to Table 1) that are key to successful IS Security processes. These are:

- The active support of management
- Sufficient funding
- Staff awareness and training.

IV. MANAGEMENT COUNTERMEASURES

Considering the importance of the security of e-government, it is urgent to dispose a whole set of effective countermeasures. The purpose is to reduce the potential risks and security bugs, so that we can reduce the risk which the e-government system environment facing.

Among the e-government risk management countermeasures, it is popular to use defense-in-depth strategy at present. Defense-in-depth strategy, exactly, is consisted of depth security and multi-level security. Through disposing multi-level security protection, we can guarantee that if one level got broken, other levels can still ensure the security of e-government system resources. For example, in case that the outer firewall of one unit got destroyed, by virtue of the inner firewall, the invader still can not get access to the sensitive data, neither commit any damage to them. Ideally, each level supplies different measures in order to avoid that the hackers can attack different levels in the same way. We have put forward an effective defense-in-defense strategy.

V. CONCLUSIONS

This work has highlighted security issues that need to be considered in designing e-government security systems. E-government services have different levels of sensitivity and they should be accessed through multiple authentication and authorization methods. The e-government security system should accommodate all clients regardless of their e-literacy levels. The system can be applied to any e-government architecture with minor adjustments. Future work includes extension to wireless technology, implementation of the system, and analysis of the system’s performance.

VI. REFERENCES


