VOL. 3, NO. 7, July 2012 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

Information Security Framework for E-Government Implementation in Nepal

[1] Pranita Upadhyaya, [2] Subarna Shakya, [3] Manish Pokharel
[1, 3] Department of Computer Science & Engineering/Kathmandu University, Kavre, Nepal.
[2] Department of E&C and Computer, Pulchowk Campus/Institute of Engineering /Tribhuvan University, Pulchowk, Lalitpur, Nepal.
[1] pranitau@yahoo.com, [2] drss@ioe.edu.np, [3] manishpokharel@gmail.com,

ABSTRACT

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. Since Nepal is an underdeveloped country whose development can be rapid through proper E-Government implementation. Presently, it is in infancy stage. One of the major failure factors identified at this stage is the improper security consideration. This paper contributes in proposing a cost effective security framework for underdeveloped country - Nepal. This paper also contributes to the e-government literature by establishing a comparative and suggestive framework for understanding, clarification and investigation of the security issues involved in improving e-government security in technologically-underdeveloped countries. It first presents a review of existing global issues of e-government security in the public sector. The paper then identifies the e-government security issues within the context of developing country - Nepal. Three cases are taken into consideration. To identify optimal solution; categorized and suggested according to their maturity levels. This is an issue which has not yet been widely addressed in the open literature.

Keywords: *E-Government, E-Services, Security, IRD, SCN, NIBL*

1. INTRODUCTION

In the rapidly growing world of ICT, various public sector organizations including e-government have focused their efforts towards digitalizing their services to their customers or citizens through the Internet so that users can easily use the available services from any place and at any time considering the fact that they are convenient to them through WWW browsers

[1],[2]. Such digitizing of information is known as e-services .However, a major concern over trust, protection and safety of such information demands a high level of security within e-government organizations. In this context, the role of e-government, trust and information security activities is to ensure confidentiality, availability, integrity, authentication and non repudiation of information in addition to providing more comprehensive understanding of user acceptance of such electronic service.

2. TECHNICAL SECURITY REQUIREMENTS FOR E-SERVICES

There exists a set of 'core' security features that may be required by an e-service application. Some of these security features are described below.

Dealing with e-Government in a comprehensive view is a big challenge and quite a complex task. With the aid of different layers, modular extensions of whole systems and the operability between different applications can be granted [10]. Several generic models are already available that address distinct issues of a complex system on different levels. Three different levels of security of e-services or Government to Citizen (G2C) have been categorized and discussed namely

a. Application layer security
b. Network layer security
c. Data security

a. Application Layer Security

According to Manish Mehta et al.[2}, The following issues are needed to be managed at this layer: Authentication , Data Integrity, Trust , User Anonymity and Security Dependencies,

The security features described above are at the service level (application level). Other Security features may be needed at lower layers in the TCP/IP suite [2],[3].

b. Network Layer Security

TCP/IP can be made secure with the help of cryptographic methods and protocols that have been developed for securing communications on the Internet. These protocols include SSL and TLS for web traffic, PGP for email, IPsec for the network layer security, MIME to expand the capacity of e-mail, S/MIME to enhance security in MIME data, Message Authentication Code to encrypt a message and Firewalls for control of access between networks, Circuit-level gateways, Application-level gateways[3],[4][9].

c. Data Security

Application-level gateways are notable for analyzing entire messages rather than individual packets of data when the data are being sent.

Some data is also confidential; not only do you not want to lose it, you don't want others to even view it without authorization. Exposure of your social security number, credit card, and bank account information could subject you to identity theft. Company documents may contain trade secrets, personal information about employees or clients, or the organization's financial records. Some ways to protect your all-important user data from loss and/or unauthorized access are required , this is done by Data Security which means protecting a database from destructive forces and the unwanted actions of unauthorized users[5],[8]. It incorporates the following measures: Back up early and often, Use file-level and share-level security, Password-protect documents, Use EFS encryption, Use disk encryption, make use of a public key infrastructure, Hide data with steganography, Protect data in transit with IP security, Secure wireless transmissions and user rights management to retain control.
The above mentioned security measures are identified for an ideal case i.e. for fully matured system. However, applying it all at the preliminary stage may be quite costly affair. Since, Nepal is an underdeveloped country where quality and cost both needs to be managed hand in hand. Optimal security requirements in every case needs to be identified i.e. before applying security measures we need to identify which level are we presently in and then propose a solution. In light of the above, there are several models called "e-Government Maturity Models (eGMMs)" developed by the international organizations, consulting firms, academia, and individual researchers with the purpose of guiding and benchmarking stage-wise e-government systems implementation and service delivery. A maturity stage in eGMM reflects the level of e-government maturity; degree of technology complexity; degree of systems sophistication; and the level of interaction with users. Also, it offers governments the abilities to measure the progress of e-government implementation [11]. Thus, in this paper we have taken three different cases for study and have tried to identify different levels of e-services based on e-Government maturity models (eGMM), Since, eGMM only provides quantitative measure[6], on the basis of it, information security Maturity Model(ISMM) are identified which outlines qualitative measure . There are a number of Information Security Maturity Models (ISMMs) developed by the international organizations, consulting firms, academia, and individual researchers with main foci on offering security services to the organizations. ISMMs proposes a structured collection of security elements needed at different levels that help organizations to easily identify and understand existing security gaps; monitor the progress of security implementation, practices, policies and quality; and monitor security investment, management and organizational audit[12];

Here, we applied the models proposed by Geoffrey Karokola et al.[6] and identified (with the help of various questioners) the gaps between the present scenario and the required security framework.

However, they are identified for global scenario, for developing/underdeveloped countries extra features like security culture, security and privacy legislation, management commitment, management style, senior management and user awareness, skills and training, management change and information security infrastructure are also to be taken care off[7].

3. RESEARCH METHODOLOGY

The research methodology used in this study is based on qualitative and quantitative methods. The process was divided into two phases. Phase one was to conduct a desk review in the area of e-government, e-government development models, and security documentations. The second phase employs a research survey where questionnaires and in depth interviews were conducted. This phase was later complemented with documentation reviews from the studied settings such as e-government strategies, and ICT security policies. Three cases were taken. Analysis were grouped based on layers discussed above. The Contacted groups were at the strategic level, tactical level and operational level. All interviewees were in one way or other responsible for delivery of e-government services to the public.*Grading is based on the set of questionnaires asked during Case Study. Multiple questions for each category were prepared. Those fulfilling all the criteria – Grade 5, with majority of the criteria –Grade 4., fulfilling half of the criteria – Grade 3.,with partial criteria – Grade -2 and with minimal criteria – Grade -1.

4. NEPAL'S SCENARIO

Various organizations have been using e-services with some preliminary security measures. Here we have chosen the better few for our case study.

a. Inland Revenue Department (IRD):

Inland Revenue Department (IRD) of Government of Nepal is currently responsible for the administration of Value Added Tax, Income Tax, and Excise Duty. Likewise, the IRD is also responsible for monitoring non-tax revenue of the government. Service is their motto and goal is to optimizing the inland revenue through fair, efficient and effective tax system. Maximizing voluntary tax compliance and providing taxpayer friendly services are their standing objectives. They provide services through 51 field offices

Types of e-services providing are E-PAN, E-TDS, E-Returns & E-SMS. According to e-government maturity models presented by Geoffrey Karokola, et al[6] ; it is at maturity level 2 –Interaction: Refer Table-1

Table 1: *eGMM Level 2 Interaction

S.No	Requirements	Available
1	Government provides enhanced interactive websites with more capabilities.	Yes
2	Websites are used as tools for interaction between government and citizens	Yes
3	Available services include search engines	Yes
4	Documents downloading, filling forms online, chart rooms, and emails.	Yes

*eGMM- e-government maturity model

Identified Critical Levels of Information Security Maturity Model (ISMM) at this stage are:

Table 2: ISMM Level 2 Defined

S.No.	Requirements	Avaialble	*Grading (out 0f 5)
1	Organizations with normal information security targets (IST) in a normal security risk environment.	Yes	1
2	Process metrics used	Yes	1
3	Security policies including awareness, visions, and strategies are reviewed and updated.	Yes	1
4	Security risk reduction mechanism to be used from technical and non-technical security threats	Yes	1

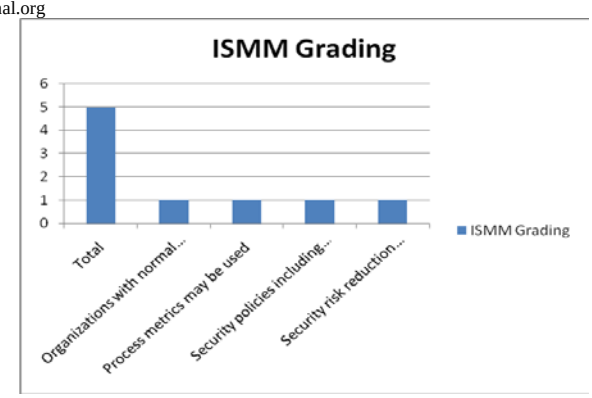

Fig 1: ISMM Grading1

b. Supreme Court of Nepal (SCN):

The Constitution provides three tiers of Court which include the Supreme Court of the Kingdom of Nepal, the Court of Appeal and the District Courts. Supreme Court is the Apex Court. There is no distinction between Criminal and Civil court except some basic procedures.

Type of e-services presently being provided are old letter management system, appeal court case management system, district court case management system, Legal information center, suggestions & complains through email at Chief Justice Office and availability of digital archive.

According to e-government maturity models (eGMM) presented by Geoffrey Karokola, et al [6], it is at maturity level 2 – Interaction (Refer Table 1 & 2) .

c. Nepal Investment Bank Limited:

Nepal Investment Bank Ltd. (NIBL), previously Nepal Indosuez Bank Ltd., was established in 1986 as a joint venture between Nepalese and French partners.

Types of e-services being provided are: Third party transfer, Utility payment, Self transfer, Statement view and internet banking. It is categorized in Maturity Stage 3 – Transaction (Refer Table 3 & 4).

Table 3: eGMM Model 3 Transaction

S.No	Requirements	Available
1	This is enhanced stage with more sophisticated technologies.	Present
2	Citizens(users) can conduct complete on-line transactions of values	Yes
3	Available services include taxes assessment and payment	Yes

Identified Critical Levels of Information Security Maturity Model (ISMM) at this stage are: Refer Table-4

Table 4: ISMM Level 3 Managed

S.No	Requirements	Available	Grading (Out 0f 5)
1	Organizations with normal information security targets (IST) in a normal/high security risk environment.	Yes	2
2	Process metrics used	Yes	2
3	Security policies including awareness, visions, and strategies are reviewed and updated.	Yes	2
4	High risk reduction mechanism to be used from technical and non-technical security threats	Yes	3

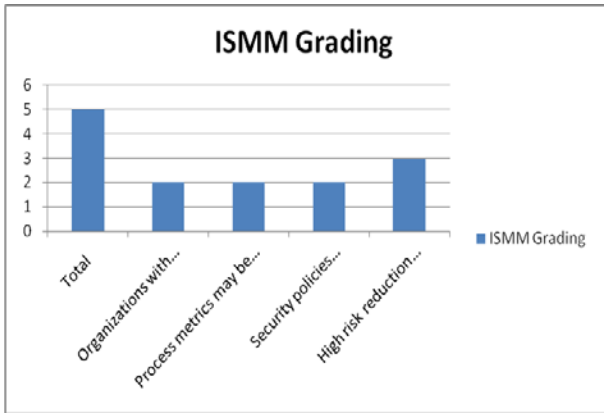

Fig 2: ISMM Grading2

5. DISCUSSION

As deduced from the tables, Nepal is lagging behind even at the initial stage of E-Government implementation as obtained from the basis of security measures taken. Out of three cases, two are in the defined level and one is at the managed level. NIBL is now heavily enhancing its ICT infrastructure and resources to meet stage three functional and operational requirements. However, they are still lagging behind from security management perspective. In short, security issues have been found neglected & may create various types of hazards.

Besides, Tables 2 & 4 depicts the global scenario. For developing countries, as suggested by Salahuddin Alfawaz et al in their paper [7]; initial indications are that, although the technology itself is essentially the same globally, environmental factors influence its application and, hence, impact on the resulting degrees of success of e-government implementations. The environmental factors identified for e- government security for developing countries are security culture, security and privacy legislation, management commitment, management style, senior management and user awareness, skills and training, management change and information security infrastructure. This too should be included in our framework.

The research findings from the three institutions revealed that Nepal has e-government implementation strategy. The latter can be propagated to the ministries, departments and agencies.
This paper contributes in proposing a cost effective Information Security Framework for E-Government Implementation in Nepal (if adapted from the beginning).

6. CONCLUSION

The majority of ICT management standards and best-practice guidelines have been developed by technologically-leading countries. The management of e-government security assurance is a relatively recent focus with which even technologically-leading countries have unresolved issues. For countries which are still developing and underdeveloped technologically, e-government security management has added issues. Looking at the existing global scenario, in Nepal there exists E-Government system but at early infancy stage. Here security should have been one of the key factors during implementation and is much lagging behind. In the absence of previous research of the sort, this paper tries to bring out the existing scenario and projects the tentative framework needed for future security measures and at the same time being cost effective.

REFERENCES

[1] Mini-track title: E-Government Trust and Information Security Issues and Concerns Track: E-Government Mini-track Chair(s):Dr Ramzi et al.

[2] Security in E-Services and Applications , Manish ehta, Sachin Singh, Yugyung Lee

[3] Rhee, M. Y. (2003). Internet Security: Cryptographic Principles, Algorithms & Protocols.

[4] IJCSNS International Journal of Computer Science and Network 2008 Security, VOL.8 No.5, May 2008 , Zhitian Zhou, Congyang Hu

[5] Information security policy British Colombia, version 2.1, March 2011, Office of the Government Chief

Information Officer Ministry of Labour, Citizens' Services and Open Government.

[6] Secure e-Government Services: Towards A Framework for Integrating IT Security Services into e-Government Maturity Models, Geoffrey Karokola, et al.

[7] E-government security in developing countries: A managerial conceptual framework; Salahuddin Alfawaz[1], Lauren May[1], Kavoos Mohanak[2]

[8] E-Government: Aspects of Security on Different Layers Maria Wimmer et. al. Institute of Applied Computer Science, University of Linz, Austria

[9] E-government Information Security: Challenges and Recommendations Wei Zhang, Computer Engineering Institute, Qingdao Technological University Qingdao 266520, P. R. China

[10] E-Government: Aspects of Security on Different Layers ,Maria Wimmer et al, Institute of Applied Computer Science, University of Linz, Austria

[11] Karokola, & L. Yngström, "Discussing e-Government Maturity Models for the Developing World – Security View". Proceedings of the 8th ISSA 2009 conference on Information Security,

[12] G. Karokola, S. Kowalski, & L. Yngström, "Towards an Information Security Maturity Models for Secure e-Government Services: A Stakeholders View". Proceedings of the 5th HAISA2011 Conference, London, UK,