E-Government Development Models: Review of Social-Technical Security Aspect

Rabia Ihmouda, and Najwa Hayaati Mohd Alwi

***Abstract*—**As the successful implementation of the e-government depends on the viable security, all the concerns related to it need to be addressed. This is because information security contributes directly to the increase in the level of trust between the government's departments and the citizens by providing an assurance of confidentiality, integrity, and availability of sensitive governmental information. E-government security is considered one of the crucial factors for achieving an advanced stage of e-government. Various types of E-government Development Models (eGDMs) have been proposed by international organizations, consulting firms, academia and individual researchers to guide and benchmark e-government implementation. The primary focus of this paper is to assess the security weaknesses of the eGDMs by reviewing seven models using Soft Systems Methodology (SSM). In line this paper provides an insight into socio-technical security aspects to create a deeper understanding of the e-government security issues, exploring and evaluating the current status and the main features of information security in eGDMs. The study is a part of an ongoing research on e-government security for the developing world. The findings show that e-government development models (eGDMs) lack built-in socio-technical security requirements.

***Keywords*—**E-governments, information security, E-Government Development Models (eGDMs), security risk, socio-technical security.

I. Introduction And Background

THE concept of an e-government is to provide access to government services anywhere at any time over open networks. Electronic government (E-government) can be considered as the use of information and communication technology (ICT), IT in order to communicate externally in the public sector (with citizens and businesses) and internally (with other government departments) [1].

The process of e-government development passes through different stages until it reaches its highest potential stage. Many e-government development models (eGDMs) that provided by international organizations and institutions and some researchers, these models include different stages that describe the development of the e-government from different perspectives.

Security has become one of the primary challenges for successful deployment of e-government. , E-government will not achieve its objectives without providing trust and security for its citizens and businesses. The confidentiality, integrity and security of data transmission and the processing need to be trusted. [2].

Despite being widely researched, the eGDMs research in itself has attracted very little study that specifically addresses the security in e-government. Further, those who did address security mentioned it en passant or focused on the transaction related security risk evident at the higher levels of the stages. This is unfortunate as "privacy and related security issues must be adequately addressed in government IT initiatives". [3]. The primary focus of this paper is to assess the socio-technical security weaknesses of the eGDMs that guide e-government implementation by reviewing seven models using SSM.

II. Security Standards And Models

While information security is an important issue to protect the data and assets of an organization, there is a need for a set of standards that help to ensure an adequate level of security to be attained, resources are used efficiently, and the best security practices are adopted. In this section we give a brief introduction to some of the most commonly used standards such as Control Objectives for Information and related Technology (COBIT), ISO 17799, and ITIL.

A. ISO standards

ISO International Standards ensure that products and services are safe, reliable and of good quality. It is issuing standards in many areas including IT and its security management systems. Implementations of these standards help organizations to effectively manage their information systems security. ISO/IEC 27002:2005 is the code of practice for information security management, which is another name of the ISO 17799 standard [4]. It provides best practices recommendations for those in charge of initiating, implementing and managing information systems security [5]. ISO/IEC 27002 contains security recommendations for 12 Security domains which include [6], [7]:

1) Security policy - management direction;
2) Organization of information security - governance of information security;
3) Asset management - inventory and classification of information assets;
4) Human resources security - security aspects of employee joining and leaving organization;

Rabia Ihmouda, Faculty of Science and Technology, Universiti Sains Islam Malaysia Bandar Baru Nilai, 71800 Nilai, Negeri Sembilan (+606-7986423 e-mail: rbhamouda@yahoo.com).

Najwa Hayaati Mohd Alwi, Faculty of Science and Technology, Universiti Sains Islam Malaysia Bandar Baru Nilai, 71800 Nilai, Negeri Sembilan(+606-7986423 e-mail: najwa@usim.edu.my).

http://dx.doi.org/10.15242/IIE.E0414057

5) Physical and environmental security - protection of computer security;
6) Communications and operations management - management of technical security;
7) Access control - restriction of access control to systems, resources and network facilities;
8) Information systems acquisition, development and maintenance - building security into applications;
9) Information security incident management - anticipating and responding to security breaches;
10) Business continuity management - protecting, maintaining and recovering business critical systems, processes and assets;
11) Compliance - ensuring compliance with organizational standards, policies, rules and regulations, procedures and norms; and
12) Risk assessment - analysis, planning, controlling and monitoring of implemented solutions and measures.

B. COBIT Standard

The Control Objectives for Information and related Technology (COBIT) is “a control framework that links IT initiatives to business requirements, organizes IT activities into a generally accepted process model, identifies the major IT resources to be leveraged and defines the management control objectives to be considered”. The latest update is version 5 by The IT Governance Institute (ITGI) [8].

COBIT is the worldwide accepted standard which prescribes areas and individual controls for IT governance, informatics and related IT processes. It provides a framework and supporting toolset that assists enterprises in achieving their objectives for the governance and management of enterprise IT. COBIT enables clear policy development and good practice for IT control throughout organizations to help enterprises to create optimal value from information technology (IT) by maintaining a balance between realizing benefits and optimizing risk levels and resource use.

COBIT enables IT to be governed and managed in a holistic manner for the entire enterprise, taking into account the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders [9].

C. ITIL (OR ISO/IEC 20000 SERIES)

The Information Technology Infrastructure Library (ITIL) is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of a business. It was developed by the United Kingdom's Office of Government Commerce (OGC), which is an international standard within the ITSM [10].

An ITIL service management is divided into the following areas [11]:

1) Service support covers one functional area, and five processes: Incident management, change management, problem management, configuration management, release management, and the service desk (Function)
2) Service delivery covers five processes: Service level management, capacity management, availability management, financial management and IT service continuity.

D. Socio-Technical Approach

The study was grounded on the theoretical foundation from the Socio-Technical approach (STA) and the Security By Consensus (SBC) model (Kowalski, 1994). Socio-technical systems theory has been used for decades as a framework to design and understand organizations.

1. Socio-Technical Model (STM)

Kowalski [12] developed Socio-technical model (STM), the model is depicted in Fig 1. The STM has two sub-systems including Social (culture and structures) and Technical (methods and machines). He argues that a change in “Machines” does not only affect the “Methods” used but also “Culture” and “Structure” as the system tries to attain balance. The changes in one sub-system may cause disturbances / disorder in other sub-systems and consequently to the entire system. This is demonstrated by the arrows linking sub-systems within sub-systems.

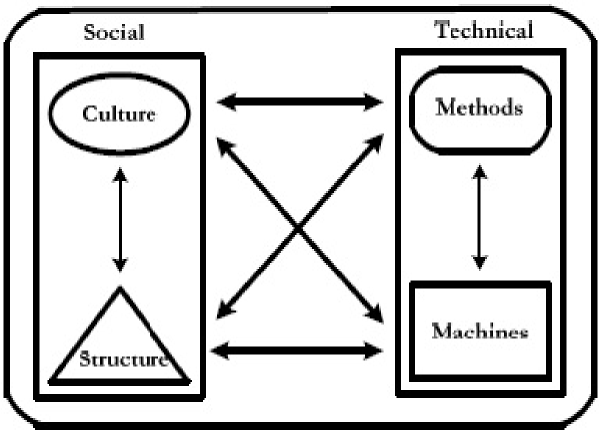

Fig 1 Socio-Technical Model (Kowalski, 1994, p.10)

2. SBC Model

To explicitly define the detailed parts of the Socio-technical Model (STM) subsystem controls – the Security By Consensus (SBC) model was applied, detailed in Fig 2.

A better model of security is the SBC model proposed by Kowalski (1994) which gives a more useful description of security [13]. The SBC model can be used to analyze security at every level, from individual to national. This flexibility combined with the inclusion of the social elements meant that the SBC-model was the best fit for this study.

The model is divided into two basic components such as a social subsystem and a technical subsystem, it is further divided into subclasses social (Ethical-cultural, Legal-contractual, Administrative-managerial-Policy, and Operational-procedural) and Technical (Mechanical-electronic and Information-Data).

http://dx.doi.org/10.15242/IIE.E0414057

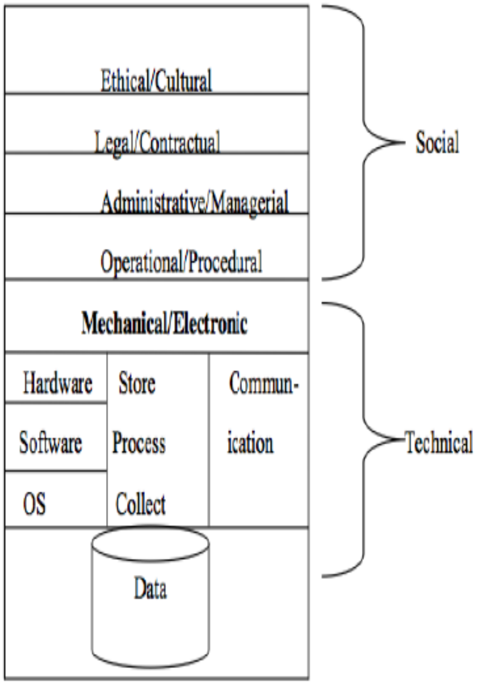

Fig. 2 The basic SBC Model Kowalski [12]

Tarimo who developed a mapping of security management domains in the ISO 17799 on the basis of the SBC model, this helps to easily comprehend security controls and issues at organizational level [14].

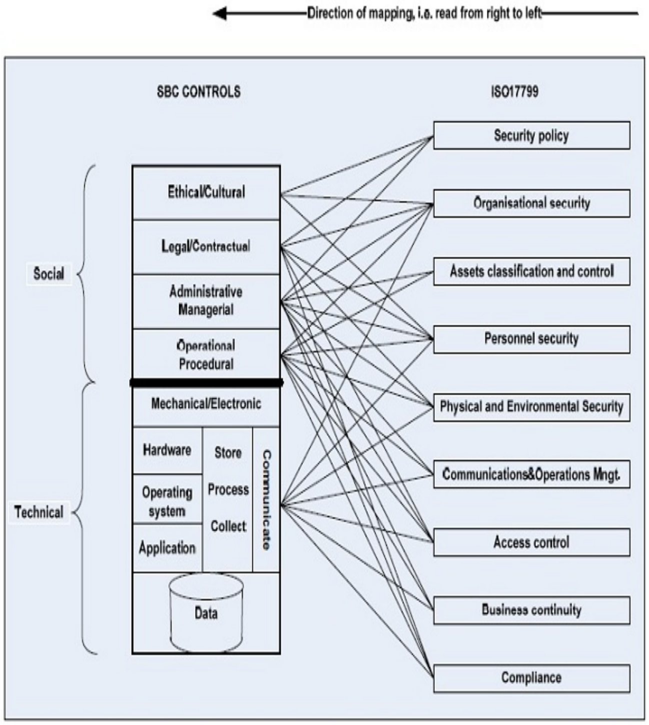

Fig. 3 Mapping the Desired ICT Security Management State (ISO 17799) onto the SBC Model Tarimo [14]

E. E-government Development Models

E-government Development Models (eGDMs) have been used not only to define the stages of development, but also to benchmark and guide its implementation and development.

To assist policymakers in devising their own plans and initiatives, some books divide the process of e-government implementation into three phases. These phases are not dependent on each other, there is no need for one phase to be completed before another can begin, but conceptually they offer ways to think about the goals of e-government [15].

Various models are briefly discussed later. We thoroughly investigated and analyzed each model for the level of available security services.

1. Layne and Lee's Model:

Layne & Lee [16] proposed a four stages model as follows: catalogue, transaction, vertical integration, and horizontal integration.

2. Siau and Long Synthesize E-government Model:

Siau & Long [17] have synthesized a new development model by combining several development models and joining the similarities. The model has four stages as follows: Interaction, Transaction, Transformation, and E-democracy.

3. Moon's Model:

Moon [18] has proposed five stages model that consist: Simple information dissemination (one way communication), Two-way communication (request and response), Service and financial transactions, Vertical and horizontal integration, and Political participation.

4. West's Model:

Darral West, proposed four stages model which consists: Billboard, the partial service-delivery, the portal with fully executable and integrated service delivery, and Interactive democracy [19].

5. Deloitte's Model:

The model is citizen-centric focused. This model has six stages as follows: Information publishing, (Official) two-way transactions, Multi-purpose portals, Portal personalization, Clustering of common services, and Full integration and enterprise transformation [20].

6. Howard's Model:

This model consist of three stages as follows: Publishing, Interacting, and finally the Transacting [21].

7. Hiller and Belanger's Model:

Hiller and Belanger proposed a five stages model as follows: Information, Two-way communication, Transaction, Integration, and Participation [22]. The model focuses on functionality, and it has considered the potential benefit of e-democracy.

III. Methodology

Soft Systems Methodology (SSM) was applied to guide this study. It is a holistic approach for analyzing complex situations in its real-world environment, and proposed solutions to the identified problem. The approach is designed in such a way that it forms repetitive cycles of scientific inquiry [23]. The steps of the methodology are:

http://dx.doi.org/10.15242/IIE.E0414057

1) Finding out about a problem situation, the identified problem in the real-world settings was insecure e-government services, which were mainly due to the lack of socio- technical security services in the eGDMs.
2) Formulating some relevant models for assisting in carrying out the study – refers to conducting extensive studies, existing documents, theories, methods and structures to understand the real-world problem. The Socio-technical model (STM) , Security By Consensus model (SBC) [12], and the ISO/IEC 27002 twelve security control principles [ISO-27k] were identified as tools for guiding the analysis.
3) Debating/analyzing the situation using the models, the analyzed of each model for the level of available security services was grounded on the theoretical foundation and building blocks from the Socio-Technical approach (STA) and the Security By Consensus (SBC) model [12]. Additionally, it utilizes the concepts ISO 27002 twelve security control principles [ISO-27K].
4) Observation step – refers to comparison and establishment of relationships between the knowledge-base and reality of the research problem

IV. Analysis Of E-Government Development Models (EGDMS)

The stage-model outlines the available services and structural transformations of governments as they progress towards an electronically-enabled government. This progress may imply fundamental changes in the form of government. In this section, seven e-government development models are described.

A. Layne and Lee's Model

When analyzing the model based on the SBC model presented in Fig 3– the model design has not addressed Ethical/ Cultural and Legal/ Contractual at the model stages. The addressed socio-technical security services controls are administrative and managerial for stages 3 and 4, and operational and procedural for stages 2, 3, and 4.

B. Siau and Long Synthesize E-government Model:

Based on the theoretical foundation presented in Fig 3 – the analysis shows that the model design has not addressed Ethical/ Cultural and Legal/ Contractual at the model stages. The model has addressed Socio-technical security services at the interaction and transaction stages (stages 2 and 3). They are addressed at the administrative and managerial, and operational and procedural controls respectively.

C. Moon's Model:

The analysis was guided by the theoretical foundation presented in Fig 3 which shows that the socio-technical security services were not addressed.

D. West's Model:

The analysis of the model is based on the concept presented in Fig 3 above which shows that the model design has not addressed Ethical/ Cultural, Legal/ Contractual and Administrative Managerial at the model stages. Socio-technical security services were addressed at the operational and procedural controls at the stages 2.

E. Deloitte's Model:

When analyzing the model based on the SBC model presented in Fig 3, the analysis shows that the model did not address the socio- technical security issues at all.

F. Howard's Model:

When analyzing the model based on the SBC model presented in Fig 3, the model design did not consider the inclusion of the Socio-technical security-related services.

G. Hiller and Belanger's Model:

Based on the analysis guided by the theoretical foundation presented in Fig 3, the socio-technical security controls were not addressed at all.

V. Discussion And Results

Table I presents the findings and an aggregation of the available socio-technical security at the models. For instance, the Table 1 shown that the Layne & Lee and Siau & Long models have not addressed Ethical/ Cultural and Legal/ Contractual at the model stages. West's model has not addressed Ethical/ Cultural, Legal/ Contractual and Administrative Managerial at the model stages.

Table 1
Summary review of STS in seven EGDMS

*EC = Ethical/ Cultural, LC= Legal/ Contractual, AM= Administrative Managerial, OP= Operational Procedural

N	The Models	No Of Stages	Social-Technical Security			
			EC	LC	AM	OP
1	Layne and Lee	4	X	X	√	√
2	Siau and Long	5	X	X	√	√
3	West	4	X	X	X	√
4	Moon	5	X	X	X	X
5	Deloitte	6	X	X	X	X
6	Howard	3	X	X	X	X
7	Hiller & Belanger	5	X	X	X	X

The socio-technical security controls were not addressed at all by Moon, Deloitte, Howard, and Hiller & Belanger models. Therefore, based on Table 1, we found that:

1) Socio-technical security requirements were not the main focus during the models' design and development.
2) Socio-technical security controls did not address the at all in some models like Moon, Deloitte, Howard and Hiller & Belanger.

The findings of the analysis for the eGDMs have showed that, these models are developed from difference perspectives. West's model and Howard's model focus on functionality and citizen-centric, Deloitte's model is focus on citizen-centric, Moon's model and Hiller's model focus on functionality, and they have consider the potential benefit for e-democracy, Layne's model is developed based on a general or an integrated perspective combining technical, organizational, and managerial feasibility, Siau's model is citizen-centric and functionality, it considers the potential benefits of e-democracy. However, the focus of those studies did not include security services.

The findings of the analysis also clearly show that the eGDMs lack built-in socio- technical security. Therefore, as the eGDMs are used to guide and benchmark e-government implementation and service delivery, it is imperative to include comprehensive security services that address socio-technical security requirements.

In this regard, the paper enhances awareness and understanding of the importance to having secure e-government services. It outlines the need of security from socio-technical aspect to be developed to match the pertinent security requirements at the e-government implementation.

VI. Conclusions and Future Work

E-government offers many benefits to government agencies, citizens and business community. However, e-Government services are prone to current and emerging security challenges posing potential threats to critical information assets. Securing it appears to be a major challenge facing governments globally. This paper reviews seven models which focus on the e-government development stages. Based on the literature review and conceptual analysis, the paper then discusses the socio-technical security weaknesses of each model based on Socio-technical model (STM), Security By Consensus model (SBC) [12], and the ISO/IEC 27002 security control principles [ISO-27k] were identified as tools for guiding the development criteria of the analysis.

The findings of the analysis for the eGDMs clearly showed that the eGDMs stages lack of socio- technical security. There is a clear need for socio-technical security to be focused onto the eGDMs stages. Further research work will include developing socio-technical security framework services/ requirements for securing the e-government implementation.

References

[1] Ebrahim, Z. and Z. Irani, E-government adoption: architecture and barriers. Business Process Management Journal, 2005. 11(5): p. 589-611. http://dx.doi.org/10.1108/14637150510619902

[2] Moosa, A. and E.M. Alsaffar. Proposing a hybrid-intelligent framework to secure e-government web applications. in Proceedings of the 2nd international conference on Theory and practice of electronic governance. 2008. ACM. http://dx.doi.org/10.1145/1509096.1509109

[3] Edwards, D.C., et al. E-Government System Security Model (eGSSM): A Multidimensional, Risk Based Approach to E-Government. in Privacy, security, risk and trust (passat), 2011 ieee third international conference on and 2011 ieee third international conference on social computing (socialcom). 2011. IEEE.

[4] Suduc, A.-M., M. Bizoi, and F.G. Filip, Audit for Information Systems Security. Informatica Economica, 2010. 14(1): p. 43-48.

[5] ISO ISO/IEC 27001:2005, Information technology -- Security techniques -- Information security management systems -- Requirements. 2005.

[6] Mandol, S., Puja and M. Verma Formulation of IT Auditing Standards. IT Audit Seminar organized by National Audit Office China, 2004.

[7] HKSAR AN OVERVIEW OF INFORMATION SECURITY STANDARDS. The Government of the Hong Kong Special Administrative Region, 2008.

[8] ITGI. IT Governance Institute. . 2013 [cited 2013 2-12-2013]; Available from: http://www.itgi.org.

[9] ISACA Information Systems Audit and Control Association. 2012.

[10] Best Management Practice. An Introductory Overview of ITIL V3, 2007.

[11] Murphy, D. Configuration Management Working Group. 2005.

[12] Kowalski, S., IT Insecurity: A Multi-disciplinary Inquiry. 1994: Univ.

[13] Nohlberg, M., Social engineering: understanding, measuring and protecting against attacks. 2007, ph. d. Licenciature, dept. Hum. And inf., univ. Of skövde, sweden.

[14] Tarimo, C.N., ICT security readiness checklist for developing countries: A social-technical approach. 2006, Stockholm.

[15] Al-Hashmi, A. and A.B. Darem, Understanding phases of E-government project. New Delhi: Retrieved from http://www. csi-sigegov. org/emerging_pdf/17_152-157. pdf, 2008.

[16] Layne, K. and J. Lee, Developing fully functional E-government: A four stage model. Government information quarterly, 2001. 18(2): p. 122-136. http://dx.doi.org/10.1016/S0740-624X(01)00066-1

[17] Siau, K. and Y. Long, Synthesizing e-government stage models–a meta-synthesis based on meta-ethnography approach. Industrial Management & Data Systems, 2005. 105(4): p. 443-458. http://dx.doi.org/10.1108/02635570510592352

[18] Moon, M.J., The Evolution of E-Government among Municipalities: Rhetoric or Reality? Public administration review, 2002. 62(4): p. 424-433. http://dx.doi.org/10.1111/0033-3352.00196

[19] West, D.M., E-Government and the Transformation of Service Delivery and Citizen Attitudes. Public administration review, 2004. 64(1): p. 15-27. http://dx.doi.org/10.1111/j.1540-6210.2004.00343.x

[20] Deloitte and Touche, The citizen as customer. CMA Management, 2001. 74(10): p. 58.

[21] Howard, M., E-government across the globe: how will'e'change government. e-Government, 2001. 90: p. 80.

[22] Hiller, J.S. and F. Belanger, Privacy strategies for electronic government. E-government, 2001. 200: p. 162-198.

[23] Checkland, P. and J. Scholes Soft Systems Methodology. 1990.