International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471
Vol. 3 Issue 6, June-2014, pp: (60-67), Impact Factor: 1.147, Available online at: www.erpublications.com

A Systematic Review on E-government Security Aspects

Rabia Ihmouda[1], Najwa Hayaati Mohd Alwi[2], Ismail Abdullah[3]
[1,2,3]Faculty of science and technology, Universiti Sains Islam Malaysia (USIM), Negeri Sembilan, Malaysia

Abstract: In recent years, most governments invested in the development of electronic government to improve government's efficiency and provide better services to businesses and citizens. While rapid growth of information and communication technology in government can facilitate improved government service it may be accompanied with many security threats. E-government security is considered as one of the most important issues for achieving an advanced stage of e-government. A higher level of e-government security is required while the number of e-government services introduced to the user increases. Computer security is not just about technology and systems. It is also about the people that use those systems and how their vulnerable behaviors can lead to exploitation. In this paper, systematic review method is applied to identifying, extracting and analyzing the security weaknesses in e-government. It is aims to show the need of the security (technical and socio-technical) requirements to be concern into the e-government implementation.

Keywords: E-government – information Security – Security issues.

1. Introduction

The advances in information and communication technology (ICT) have made many electronic services possible. This revolution is not only changing the daily lives of people but is also changing the characteristics of interactions between governments and citizens. These changes, in turn, are rapidly being transformed into new forms of government named electronic government (e-government). Indeed, with many Information Technology (IT) applications such as electronic commerce, e-learning, and accompanying stories of success and failure, it is inevitable to participate in the e-government movement [1]. Electronic Government, or e-Government and its many synonyms, has been on the international agenda for several years. Since the late 1990s, governments at all levels have launched e-government projects in order to provide electronic information and services to citizens and businesses [2]. The concept of an e-government is to provide access to government services anywhere at any time over open networks. E-government can be defined as government use of IT in order to communicate externally in the public sector (with citizens and businesses) and internally (with other government departments) [3].

The term 'Security' generally refers to the protection of information system assets and control of access to information. Without the assurance of security to the privacy nobody would be prompted to use e-government. E-government is the using of information technology to break the boundary of administrative organizations, and build up a virtual e-government, public and private organizations are facing a wide range of information threats, information security is a crucial factor in their information systems [4]. Information security is a serious requirement which must be carefully considered, not as an isolated aspect, but as an element presented in all stages of the development lifecycle, from requirement analysis to implementation and maintenance [5], [6]. In this way, information assurance, security and privacy have moved from being considered by information systems designers as narrow topics of interest to become critical issues of fundamental importance in our society [7].

E-government services create new security challenges to government, business and citizens. Therefore an increased variety of security services is required [8], [9], [10], [11], [12]. The first issues on security coming in mind regard of course technical aspects. Security aspects not only regard technical issues. Instead, these need careful investigation from a socio-technical viewpoint as well [13]. In this paper, we will carry out a systematic review of the existing literature on e-government security weaknesses with the objective of knowing, study and analyzing the most relevant literature. To perform this systematic review, the study on the guideline proposed by Kitchenham [14] that is appropriate for software engineering researchers. In addition, it use a review protocol template developed by Biolchini et al [15] which facilitates systematic reviews planning and execution in software engineering.

2. Systematic Review Approach

The systematic review process conduction can be understood as a three-step approach (Fig 1). The first phase of the research starts from concepts, which explicitly and formally represent the issue in question, and goes to studies, which

material potentially contains the information that provide evidence about dissected in their contents, compared among themselves, and sometimes reassembled in their constituent parts, leading to results, which represent the emergence of a new type of evidence. The third phase goes from these results, through a process of analysis and synthesis of the new arrangements of data that are made possible through this methodology, towards the conclusions, which implicate in acquiring new knowledge about the issue in question as well as supporting some decision making related to it.

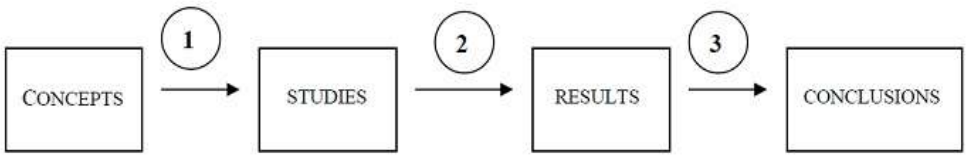

Figure 1. The systematic Review Three-Step Approach.

2.1 Systematic Review procedure

The study used a review protocol template developed by Biolchini et al [15] which facilitates systematic reviews planning and execution in software engineering.

2.1.1 Review Planning

In this phase, it must define the research objectives and the way in which the review will be executed, which includes the formulations of research questions and the planning of how the sources and studies selection will be carried out.

- Question Formularization: The research objectives must be clearly defined in this section. The question focus is to identify the most relevant works regard of the security in e-government implementation, In section 1, we have presented security as a relevant aspect to be taken into account in the e-government implementation. The research question which will be addressed by our research is the following one: What the security weaknesses in e-government project? The keywords and related concepts that make up this question and that will be used during the review execution are:

- e-government security
- Security (Secure).
- Social- technical security

In the context of the planned systematic review, the e-government security literatures will be observed and analyzed. And therefore, the population group that will be observed is formed by publications in the selected data sources. The expected result at the end of this systematic review is the identification of the weaknesses related to e-government security.

- Sources Selection: The objective of this section is to select the sources where searches for primary studies will be executed. The selection criteria to evaluate studies sources are based on the opinion of the authors of this work. Besides, these sources must be web available and must be written in English. The following list of sources has been considered: ScienceDirect, ACM digital library, IEEE digital library, Scholar Google.

- Studies Selection: Once the sources had been defined, it is necessary to describe the process and the criteria for studies selection and evaluation. The inclusion and exclusion criteria of this study were based on the research question. We therefore established that the studies must contain issues and topics which consider security on e-government, and must describe threats, vulnerabilities, weaknesses, and risks.

2.1.2 Review Execution

During this phase, the search in the defined sources must be executed and the obtained studies must be evaluated according to the established criteria. In next section, the information relevant to the research question must be extracted from the selected studies. The obtained studies which completely fit all previously defined inclusion and exclusion criteria are the following ones:

Table : 1 Study Selection

Author	Title
Moen, et al	Vulnerabilities in e-governments
Cenzic	Web Application Security Trends Report Q3-Q4
Maple & Phillips	UK security breach investigations report: an analysis of data compromise cases
Bagchi & Udo	An analysis of the growth of computer and Internet security breaches

Gordon, et al	2004 CSI/FBI computer crime and security survey
CyberSecurity Malaysia	H1 2013: Cyber security scene in Malaysia
CNN.	Chinese hackers attacked crucial government election website
E Hacking News.	Kerala Government websites hacked by Syrian Hacker 'Dr.SHA6H'
Wang, J.-f.	E-government security management: key factors and countermeasure
NW3C.	Internet Crime Report 2012
Ponemon,	2013 Cost of Cyber Crime Study: United State
PwC.	Key findings from the 2013 US State of Cybercrime Survey
Ihmouda & Mohd Alwi	PENETRATION TESTING FOR LIBYAN GOVERNMENT WEBSITE
ITGI.	IT Governance Institute
Kowalski, S.	IT Insecurity: A Multi-disciplinary Inquiry
Gil-García & Pardo,	E-government success factors: Mapping practical tools to theoretical foundations
Martins, & Elofe	Information security culture
Michael, et al	Principles of Information Security
Wimmer & Von Bredow	A holistic approach for providing security solutions in e-government
Wimmer & Von Bredow	E-government: Aspects of security on different layers
Conklin, W. A.	Barriers to Adoption of e-Government. Paper presented at the System Sciences
Ebrahim, & Irani,	E-government adoption: architecture and barriers
May & Lane	A Model for Improving e-Security in Australian Universities
Siponen & Oinas-Kukkonen	A review of information security issues and respective research contributions
Bostrom, & Heinen,	MIS problems and failures: A socio-technical perspective, Part II: The application of socio-technical theory
Kling, & Lamb,	IT and organizational change in digital economies: a socio-technical approach
Damodaran,et al	The contribution of sociotechnical systems thinking to the effective adoption of e-government and the enhancement of democracy
Dawes, S. S.	Governance in the digital age: A research and action framework for an uncertain future
Briney & Prince	Does Size Matter. Information Security
Dhillon & Backhouse	Technical opinion: Information system security management in the new millennium
Höne & Eloff,	Information security policy—what do international information security standards say?
Ives et al	A framework for research in computer-based management information systems
Alfawaz, et al	E-government security in developing countries: A managerial conceptual framework
Layne & Lee	Developing fully functional E-government: A four stage model. Government
Siau, & Long,	Synthesizing e-government stage models–a meta-synthesis based on meta-ethnography approach
Moon	The Evolution of E- Government among Municipalities: Rhetoric or Reality?
West, D. M.	E- Government and the Transformation of Service Delivery and Citizen Attitudes
Deloitte, & Touche.	The citizen as customer
Howard, M.	E-government across the globe: how will ' e' change government?
Hiller & Belanger	Privacy strategies for electronic government
Brancheau, et al	Key Issues in Information Systems Management: 1994-95 SIM Delphi Results
Hong, et al	An integrated system theory of information security management
Kotulic & Clark	Why there aren't more information security research studies
Wood, C. C.	A management view of Internet electronic commerce security
Whitman, M. E.	In defense of the realm: understanding the threats to information security
Vermeulen & Von Solms	The information security management toolbox–taking the pain out of security management
Foltz, et al	Have you met your organization's computer usage policy?

2.1.3 Information Extraction

In this section, extraction criteria and results will be described. The selected areas to classify studies are as follows:

- Security incident reports in e-government.
- Recent literature focusing on e-government security from technical and socio-technical aspects.

Next, we will present a brief outline of each of the selected studies in the previous section we will only focus on e-government security weaknesses (technical and socio- technical) aspects due to space constraints to show the needed of the security requirements to be concern into e-government implementation.

- **Technical security aspect**

Moen et al [16] stated that the majority of the dynamic E-Government Web applications had vulnerabilities exploitable by Cross Site Scripting (XSS) or SQL injection. Therefore, the importance of information security can not be ignoring. Even if the issue of information security is not new, most of the organizations are facing growing number of challenges and threats due to changing, and risky environments around the globe.

The web is becoming a dominant threat to computer security. In the second half of 2009, 82% of the reported commercial vulnerabilities were related to web technologies (higher than 78% in the first half of the 2009) [17]. Maple and Phillips [18], in the report of the cases investigated by SAFE UK, 86% of the attacks exploited vulnerability in the web interface, while only 14% targeted other parts of the infrastructure. Attackers know that valuable data passes through the web, and the web interface is accessible to outsiders, thus making the web a logical point of attack.

In the world of cyber warfare, while government websites are becoming increasingly prone to numerous threats which make the issue of security of various sensitive government data a great challenge for the government organizations. Increasing attention is given to the security related issues of these websites and every attempt is made by these organizations to ensure the adequate protection of their sensitive information [19]. This is because findings of various national surveys confirm a high number of cyber attacks against the information resources of such organizations [20], [21]. Therefore, in the changing nature of the warfare, the need to secure the information and minimize the risk is becoming more important than ever before.

Malaysian National Agency [22] reported that the increase of reported 5,592 cyber security incidents in the first of half 2013 is in tandem with the enhanced use of ICT as a key economic driver towards developed nation status by 2020. The report from the Center for Public Integrity, one of the country's oldest and largest nonpartisan, nonprofit investigative news organizations, indicates that Chinese hackers crashed the FEC's computer systems, they tapped into the Federal Election Commission's website during the federal government shutdown in October, which compiles federal election campaign finance information like contributions to parties and candidates, and how those billions of dollars are spent in each election by candidates, political parties, and independent groups such as political action committees [23].

The report by Sabari Selvan on Sunday, December 08, 2013 - A Syrian Hacker using online handle 'Dr.SHA6H' who is known for his Government websites' hack, now started targeting Indian Government websites, he hacked into a number of Indian Government sites and left them defaced [24]. The National Computer Network Emergency Response Technical Team/Coordination Center of China (CERT) in 2007 have received 26476 network security incident reports, it was three times more than 2005 which was reported 9122 network security incidents [4]. The wave of cyber crimes has increased at an alarming rate worldwide leaving millions of victims in its wake each day. And the costing was growing as mention in the some following reports in Table II.

Table 2 : The cyber crimes cost

In 2012, The Internet Crime Complaint Center (IC3) [25].	received 289,874 consumer complaints,	$525,441,1101 dollar loss
Ponemon Institute© Research Report 2013[26]	The companies in their study experienced 122 successful attacks per week	the average annualized cost of cyber crime for 60 organizations in their study is $11.6 million per year, with a range of $1.3 million to $58 million.
Malaysia police: $1.1M lost through cyber hacking this year [22]	They have recorded 24 cases of electronic hacking cases between January and September	The losses amounting to 3.3 million ringgit (US$1.1 million). The country lost 2.75 billion ringgit (US$897.6M) over the past five years to cybercrime with the financial sector being hit the hardest.
PwC [27]	IP theft was growing	Costing the United States more than $300 billion each year.

Ihmouda and Mohd Alwi [28] stated that there is an urgent need to address the information security vulnerabilities and weaknesses in the government by developing a security framework of nation standards for e-government. As discussed in the earlier, the e-government implementation faces various issues related to security and data protection. The major concern in this respect of security is related to technical aspects. Today, a vast body of research is available on this aspect and a lot of research has been to provide secure transactions, to offer protection against hacker and various cyber attacks

etc. however, the Information Systems (IS) security is a critical issue facing organizations worldwide today. Therefore, there is an increased need to focus on this information protection and security related to technical aspects [29]

.

- **Socio-Technical security aspect**

Security threats posed to e-government services could result from technical and/or socio-technical related issues. Technical security aspects may include vulnerability caused by poor system design, development, implementation, configuration, integration (vertical and horizontal), and/or maintenance. Similarly, socio-technical security aspects may result from lack of ethical and cultural norms, legal and contractual documents, administrative and managerial policies, operational and procedural guidelines, and/or awareness program [30], [31], [32], [33], [12]. Until now, a lot of technical security solutions and architectures exist within the scope of IT. Efforts mainly concentrate on certain aspects or functionality of security such as digital signatures, PKI-infrastructures, firewalls or anti-virus mechanisms. But security issues not only concern technical matters. Aspects of trust, legal issues, privacy, authentication, confidentiality etc. need to be solved as well [13].

Data from The Software Engineering Institute CERT® Program at Carnegie Mellon University Insider Threat Database, a repository of reported insider threat cases involving theft of IP using IT, IT sabotage, or fraud using IT, shows that 27% of the incidents in the database were detected by socio-technical means. As an FBI insider threat analyst explained this at the February 2013 RSA conference, "…the risk from insider threats is not a technical problem, but a people centric problem. So you have to look for a people-centric solution. People are multidimensional, so what you have to do is take a multidisciplinary approach."[27].

Articles on e-government have been published in some leading countries 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 issues and socio-technical issues should be considered when implementing e-government [4]. Sense information security involves people as well as technologies. A small number of studies in the literature that address the social acceptance of security technologies, known as the organizational security culture [34], [35]. The existing studies have shown that socio-technical issues are as important as technical issues to secure an organization's sensitive information, and there are invested in developing technical security services more than socio-technical security ones [36] [35].

Socio-technical theory is widely regarded as the key to information systems success [37]. The high failure rate of many information systems (IS) is often due to considering information technology (IT) as a tool instead of as socio-technical system [38], with an objective of delivering a sound technical system without taking into considerations the necessary organizational and social environment in which the technical system must operate. In the context of e-government, several researchers assert the need for incorporating socio-technical approaches in designing and delivering e-government services [39], [40]. For example, Damodaran et al, stated that e-government service delivery according to the needs of the citizens ''requires the development of socio-technical sub-systems, combining technology and communication processes which meet the task needs of citizens and the procedural and legal requirements of local government''. Dawes, while presenting an e-government framework, asserted that in addition to tools and technologies, governments must take into account values and policies, and human, organizational, institutional, and societal factors; an infrastructure that suit future e-government.

According to a survey conducted by Briney and Prince [41], the most pressing problems on information security The survey result showed that most information security problems were caused by the negligence of people, rather by attack events. Therefore, it is important to train and manage the problem-prone people. There are several models of information security based on the concept of the socio-technical approach in the literature. Dhillon and Backhouse [42] discusses how socio-technical system approaches can be combined with usability engineering in the design of information systems. The Security By Consensus (SBC) model has been suggested by Kowalski [30], 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). Höne and Eloff [43] argue that an information security management system (ISMS) consists of many aspects such as technology, policies, guidelines, codes of practice, standards, human issues, legal and ethical issues. Ives et al [44] proposed comprehensive Management Information Systems (MIS) research model, the model is to understanding and classifying MIS research. It is widely known and discussed in the information system management literature.

To a large extent technological solutions for the majority of security issues have been previously developed. There are however still many application challenges, the people and processes components of information assurance management. This leads to the need for the socio-technical approach to focusing on these issues. In today's Information Age this is a very topical issue which is yet to be widely addressed [45]. To guide and benchmark e-government implementation and

service delivery, international organizations, consulting firms, academia and individual researchers have proposed various types of e-government development models (eGDMs). These models outline different stages that a government can follow in order to offer the best and most efficient e-government services [46], [47].

Layne and Lee [1] proposed a four-stage model. The stages are catalogue, transaction, vertical integration, and horizontal integration, this model based on technical, organizational, and managerial feasibility. Siau and Long,[48] have synthesized a new development model from different models using the meta-synthesize method, which is relatively new in the field of information technology. By combining several development models and joining the similarities; the four stage model has the following stages: Interaction stage, Transaction stage, Transformation stage, and E-democracy stage (v) E-democracy. Moon [47] has submitted his development model, which has five stages as follows: Simple information dissemination (one way communication) stage, Two-way communication (request and response) stage, Service and financial transactions stage, Vertical and horizontal integration stage, and Political participation stage. Darral West proposed model that consists of four stages as follows: Billboard stage, the partial service-delivery stage, the portal stage with fully executable and integrated service delivery, and Interactive democracy stage [49]. Deloitte & Touche developed model which consists of six-stag as follows: Information publishing stage, (Official) two-way transactions stage, Multi-purpose portals stage, Portal personalization stage, Clustering of common services stage, and Full integration and enterprise transformation stage [50]. The model is citizen-centric focused. Howard developed a three stage model. The stages of the model as follows: Publishing stage_ this is the initial stage, Interacting stage_ this is the advanced stage, and finally Transacting stage based on the model design -this is the highest stage of e-government development [51]. Hiller and Belanger identified a five-stage model as follows: Information stage, Two-way communication stage, Transaction stage, Integration stage, and Participation stage [52]. The model focuses on functionality, and it has considered the potential benefit of e-democracy.

Table 3 : The e-government development models concept.

No	The model	The model proposed
1	Layne & Lee's Model	developed based on a general or an integrated perspective combining technical, organizational, and managerial feasibility
2	Siau & Long Synthesize's Model	focuses on citizen-centric and functionality, it considers the potential benefits of e-democracy
3	Moon's Model	focuses on functionality and it has considered the potential benefit of e-democracy
4	West's Model	focuses on functionality and citizen-centric
5	Deloitte's Model	focuses on citizen-centric
6	Howard's Model	focuses on functionality and citizen-centric
7	Hiller & Belanger's Model	focuses on functionality and it has considered the potential benefit of e-democracy

These models are developed from difference perspectives. West's model, Howard's model focuses on functionality and citizen-centric, Deloitte's model is citizen-centric focused, Moon's model and Hiller's model focuses on functionality, and it has considered the potential benefit of e-democracy, Layne's model 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, Security services requirements were not the main foci during the models' design and development. Based on the criteria of these models we found that eGDMs stages lack of security requirements, therefore, there is a need for security requirements to be focus onto eGDMs stages.

2.2 Result Analysis and Discuses

With increase use in e-government services on the Internet, the security related issues are also coming in the forefront. Government organizations are facing a number of challenges when offering suitable variety of secure e-government services.
E-government implementation faces various issues related to security and data protection, there are many governmental portals were subject to hacking. Therefore, **there is an increased need to focus on this information protection and security related to technical aspect**.

While many researchers dedicated their efforts to various areas of security researches, most of them focus on the technical side. Management attention to information security has been low compared to other information security issues [53], [54], and a lack of empirical research in the area of security risk management has been concluded due to the highly intrusive nature of ISM research approaches [55]. Some researches attempted to study ISM issues from managerial

perspective by interview method and tried to figure out their "professed" key success factors [56], [57], and some other articles emphasized the benefits of carrying out ISM but they ignored the prerequisite for ISM [58], [59]. **Therefore the security issues related to the people and processes components of information assurance management need to be focus. This leads to the need for the socio-technical approach to focusing on these issues.**

There are many eGDMs have been proposed to guide and benchmark e-government implementation and service delivery. Focusing on the security related challenges faced by e-government, e-government faces many security risks and challenges. Security services requirements were not the main foci during the models' design and development. **The review of these eGDMs has showed that eGDMs stages lack of security requirements, therefore, there is a need for security requirements to be focus onto eGDMs stages.**

3. Conclusions

The global IT revolution is growing rapidly. Governments and businesses have to be ready to meet the increased demand of effective and secure online services. Providing secure online services in e-government requires. This study explored the security weaknesses on e-government services. The overall results show that the lack of security is the most common problem faced by many e-government projects. In this regard, the paper enhances awareness and understanding of the importance to having secure e-government services, it outlines the need of security requirements to be developed at the e-government implementation. There is an urgent need to address the information security vulnerabilities and weaknesses in the government by developing a security framework of nation standards for government. The framework would assist them in mitigating the current and emerging security risks and threats posed to e-government services.

4. References

[1]. Layne, K. and J. Lee, Developing fully functional E-government: A four stage model. Government information quarterly, 2001. 18(2): p. 122-136.
[2]. Tat-Kei Ho, A., Reinventing Local Governments and the E-Government Initiative. Public administration review, 2002. 62(4): p. 434-444.
[3]. Ebrahim, Z. and Z. Irani, E-government adoption: architecture and barriers. Business Process Management Journal, 2005. 11(5): p. 589-611.
[4]. Wang, J.-f. E-government security management: key factors and countermeasure. in Proceedings of the 2009 Fifth International Conference on Information Assurance and Security-Volume 02. 2009. IEEE Computer Society.
[5]. Devanbu, P.T. and S. Stubblebine. Software engineering for security: a roadmap. in Proceedings of the Conference on the Future of Software Engineering. 2000. ACM.
[6]. Ferrari, E. and B. Thuraisingham, Secure database systems. Advanced databases: technology and design. Artech House, 2000.
[7]. Denker, G., L. Kagal, and T. Finin, Security in the Semantic Web using OWL. Information Security Technical Report, 2005. 10(1): p. 51-58.
[8]. Basu, S., E-government and developing countries: an overview. International Review of Law, Computers & Technology, 2004. 18(1): p. 109-132.
[9]. Grant, G. and D. Chau, Developing a generic framework for e-government. Journal of Global Information Management (JGIM), 2005. 13(1): p. 1-30.
[10]. Hwang, M.-S., et al., Challenges in e-government and security of information. Information & Security: An International Journal, 2004. 15(1): p. 9-20.
[11]. Lambrinoudakis, C., et al., Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy. Computer Communications, 2003. 26(16): p. 1873-1883.
[12]. Wimmer, M. and B. Von Bredow. A holistic approach for providing security solutions in e-government. in System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on. 2002. IEEE.
[13]. Wimmer, M. and B. von Bredow. E-government: Aspects of security on different layers. in Database and Expert Systems Applications, 2001. Proceedings. 12th International Workshop on. 2001. IEEE.
[14]. Kitchenham, B., Procedures for performing systematic reviews. Keele, UK, Keele University, 2004. 33: p. 2004.
[15]. Biolchini, J., et al., Systematic review in software engineering. System Engineering and Computer Science Department COPPE/UFRJ, Technical Report ES, 2005. 679(05).
[16]. Moen, V., et al., Vulnerabilities in e-governments. International Journal of Electronic Security and Digital Forensics, 2007. 1(1): p. 89-100.
[17]. Cenzic, Web Application Security Trends Report Q3-Q4, 2009 2009.
[18]. Maple, C. and A. Phillips, UK security breach investigations report: an analysis of data compromise cases. 2010.
[19]. Saint-Germain, R., Information security management best practice based on ISO/IEC 17799. Information Management Journal, 2005. 39(4): p. 60-66.
[20]. Bagchi, K. and G. Udo, An analysis of the growth of computer and Internet security breaches. Communications of the Association for Information Systems (Volume 12, 2003), 2003. 684: p. 700.
[21]. Gordon, L.A., et al., 2004 CSI/FBI computer crime and security survey. Computer Security Journal, 2004. 20(3): p. 33-51.
[22]. CyberSecurity Malaysia. 2013 20-11-2013]; Available from: http://www.cybersecurity.my/bahasa/ knowledge_bank /news/2013/main/detail/2318/index.html.

[23]. CNN. Chinese hackers attacked crucial government election website. 2013 22-12-2013]; Available from: http://politicalticker.blogs.cnn.com/2013/12/17/report-chinese-hackers-attacked-crucial-government-election-website/.
[24]. E Hacking News. Kerala Government websites hacked by Syrian Hacker 'Dr.SHA6H'. 2013 23-12-2013]; Available from: http://www.ehackingnews.com/2013/12/kerala-government-websites-hacked-by.html.
[25]. NW3C Internet Crime Report 2012. 2013.
[26]. Ponemon, I. 2013 Cost of Cyber Crime Study: United States 2013; Available from: http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf.
[27]. PwC, Key findings from the 2013 US State of Cybercrime Survey. 2013: US.
[28]. Ihmouda, R.H. and N.H. Mohd Alwi. PENETRATION TESTING FOR LIBYAN GOVERNMENT WEBSITE. in Proceedings of the 4th International Conference on Computing and Informatics, ICOCI 2013 28-29 August, 2013. 2013. Sarawak, Malaysia. Universiti Utara Malaysia (http://www.uum.edu.my): Universiti Utara Malaysia (http://www.uum.edu.my).
[29]. ITGI. IT Governance Institute. . 2013 [cited 2013 2-12-2013]; Available from: http://www.itgi.org.
[30]. Kowalski, S., IT Insecurity: A Multi-disciplinary Inquiry. 1994: Univ.
[31]. Gil-García, J.R. and T.A. Pardo, E-government success factors: Mapping practical tools to theoretical foundations. Government Information Quarterly, 2005. 22(2): p. 187-216.
[32]. A. Martins and J. Elofe. Information security culture. . in Proceedings of IFIP TC11, 17th international conference on information security (SEC2002). 2002. Cairo, Egypt.: Springer US.
[33]. Michael, Whitman, and H.J. Mattord, Principles of Information Security,. 3rd Edition ed. 2007.
[34]. May, L. and T. Lane, A Model for Improving e-Security in Australian Universities. JTAER, 2006. 1(2): p. 90-96.
[35]. Siponen, M.T. and H. Oinas-Kukkonen, A review of information security issues and respective research contributions. ACM Sigmis Database, 2007. 38(1): p. 60-80.
[36]. Dhillon, G., G. Tejay, and W. Hong. Identifying governance dimensions to evaluate information systems security in organizations. in System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on. 2007. IEEE.
[37]. Bostrom, R.P. and J.S. Heinen, MIS problems and failures: A socio-technical perspective, Part II: The application of socio-technical theory. MIS quarterly, 1977: p. 11-28.
[38]. Kling, R. and R. Lamb, IT and organizational change in digital economies: a socio-technical approach. ACM SIGCAS Computers and Society, 1999. 29(3): p. 17-25.
[39]. Damodaran, L., et al., The contribution of sociotechnical systems thinking to the effective adoption of e-government and the enhancement of democracy. The electronic journal of e-Government, 2005. 3(1): p. 1-12.
[40]. Dawes, S.S., Governance in the digital age: A research and action framework for an uncertain future. Government Information Quarterly, 2009. 26(2): p. 257-264.
[41]. Briney, A. and F. Prince, Does Size Matter. Information Security, 2002. 5(9): p. 36-39.
[42]. Dhillon, G. and J. Backhouse, Technical opinion: Information system security management in the new millennium. Communications of the ACM, 2000. 43(7): p. 125-128.
[43]. Höne, K. and J.H.P. Eloff, Information security policy—what do international information security standards say? Computers & Security, 2002. 21(5): p. 402-409.
[44]. Ives, B., S. Hamilton, and G.B. Davis, A framework for research in computer-based management information systems. Management science, 1980. 26(9): p. 910-934.
[45]. Alfawaz, S., L.J. May, and K. Mohannak, E-government security in developing countries: A managerial conceptual framework. 2008.
[46]. Grönlund, Å. and T.A. Horan, Introducing e-gov: history, definitions, and issues. Communications of the Association for Information Systems, 2004. 15(2004): p. 713-729.
[47]. Moon, M.J., The Evolution of E-Government among Municipalities: Rhetoric or Reality? Public administration review, 2002. 62(4): p. 424-433.
[48]. 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.
[49]. West, D.M., E-Government and the Transformation of Service Delivery and Citizen Attitudes. Public administration review, 2004. 64(1): p. 15-27.
[50]. Deloitte and Touche, The citizen as customer. CMA Management, 2001. 74(10): p. 58.
[51]. Howard, M., E-government across the globe: how will'e'change government. e-Government, 2001. 90: p. 80.
[52]. Hiller, J.S. and F. Belanger, Privacy strategies for electronic government. E-government, 2001. 200: p. 162-198.
[53]. Brancheau, J.C., B.D. Janz, and J.C. Wetherbe, Key Issues in Information Systems Management: 1994-95 SIM Delphi Results. Mis Quarterly, 1996. 20(2).
[54]. Hong, K.-S., et al., An integrated system theory of information security management. Information Management & Computer Security, 2003. 11(5): p. 243-248.
[55]. Kotulic, A.G. and J.G. Clark, Why there aren't more information security research studies. Information & Management, 2004. 41(5): p. 597-607.
[56]. Wood, C.C., A management view of Internet electronic commerce security. Computers & Security, 1997. 16(4): p. 316-320.
[57]. Whitman, M.E., In defense of the realm: understanding the threats to information security. International Journal of Information Management, 2004. 24(1): p. 43-57.
[58]. Vermeulen, C. and R. Von Solms, The information security management toolbox–taking the pain out of security management. Information Management & Computer Security, 2002. 10(3): p. 119-125.
[59]. Foltz, C.B., T.P. Cronan, and T.W. Jones, Have you met your organization's computer usage policy? Industrial Management & Data Systems, 2005. 105(2): p. 137-146.