Municipal E-Government Security: A Literature Review and Research Agenda

ABSTRACT

In recent years, electronic government (e-government) has been a topic of heighten importance and research interest within the information systems and public administration research communities. This paper seeks to develop an increased interest in e-government security for city and municipal government agencies. It provides a literature review of relevant publications and develops a case for enhanced research in this area. Furthermore it provides details upon an in progress case study in this emergent area and sets forth a research agenda for additional research avenues in municipal e-government security.

Keywords

E-government, electronic government, municipal government security, city government security, e-government research agenda

INTRODUCTION

Electronic government or e-government is not a new topic, but is one of high interest to both the information systems and public administration research communities. From a business perspective organizations realize that in order to maintain a competitive edge and reduce costs technology must be leveraged to its fullest to streamline business operations (Marchionini et al. 2003). As such, organizations now put themselves in greater contact with their customers through corporate websites, portals and integrated voice response (IVR) systems among others (Ho 2002). This exposure subjects organizations to greater probabilities of security breaches and places an additional need to focus on the security of such systems.

The trend to incorporate online services to enhance accessibility and reduce overhead costs has prompted the growth of e-government services in government agencies of all sizes. Although typically criticized for their inefficient and slow adoption of technology, government entities have employed such systems to provide better service to their constituents (Hazlett et al. 2003). This can be seen at all levels of government: federal, state and local. At the federal level the Internal Revenue Service (IRS) utilizes the web to allow tax payers to check the status of their refunds, apply for an employer

identification number (EIN) and pay taxes online, just to mention a few. In California, the Department of Motors Vehicles (DMV) provides for online vehicle registration and online booking of DMV appointments. Local municipalities are no exception either. Many cities provide several online services to their residents for items such as: filing a noise complaint, code enforcement violations and paying business license taxes.

The collection of online services provided by government is typically referred to as electronic government or e-government. The types of service provided by a given agency vary from locality and the level of government offering the service. Nonetheless, the trend can be seen that government entities are aware of the versatility and practicality of implementing online services to serve the public community (Scherlis et al. 2003). Citizens enjoy the ability of being empowered with the ability to perform various governmental activities without having to leave the comfort of their homes. This avoids long lines and hold times on the telephone to speak to a representative (Welch et al. 2005). At a first glance, all these e-government services seem like a win-win for both government and citizens.

However, increased exposure also increases the security risks for agencies. The increase in identify theft, terrorist attacks and security breaches has emphasized the importance of information security (Taylor 2002). Large federal and state agencies are subject to more regulation and oversight than municipal levels of government. However, many municipal or local government entities are not provided with the necessary resources or regulation to maintain secure e-government services.

This paper seeks to shed light on the information security capabilities and resources of municipal government entities. It provides a literature review of pertinent publications and furnishes details of an in progress descriptive case study in the area. Lastly, it develops a research agenda for additional research and publication.

The in progress case study mentioned earlier will focus on (3) three primary research questions:

RQ1: What level of e-government security do municipalities currently have when benchmarked to federal e-government security requirements?

RQ2: How can municipal agencies reach a federal level of e-government security?

RQ3: Why are municipalities not fully compliant with federal e-government security requirements?

The E-Government Act of 2002 has a key provision directly relating to federal e-government security: Security Protocols to Protect Information. Municipal government agencies are not required to adhere to these security requirements.

However, this case study will investigate which of these requirements municipal government entities are compliant with and also seek to identify how they can become more compliant.

LITERATURE REVIEW

A literature review has been conducted to highlight the importance and need for security within e-government offerings. In preparing this literature review, care was exhibited to ensure that the initial literature review was not too extensive as to hamper the ability to adequately theorize over the potential findings as recommended by Glaser and Strauss (1968).

To search for pertinent articles relating to e-government and security, several online resources were utilized. Literature was obtained from the following databases: ABI/INFORM, ProQuest, eBSCO Host, ACM Library and InfoSECURITY. This initial literature search yielded a total of over 100 articles, journals and abstract sources. The abstracts or overviews were reviewed to determine their applicability to the topic. The following criteria were used to determine the applicability for the purposes of this study:

1) Research paper had a primary focus of e-government
2) Focused on the use, implementation or effects of e-government
3) Excluded papers having a primary focus of e-voting systems
4) Relevance to research topic

The sources were then reduced to more manageable count of 19, of which had the highest relevance to the research topic. The distribution of these sources is shown below in Table 1.

Table 1 – Distribution of E-Government Literary Sources

Literature Review - Sources by Discipline		
Business, Management and Public Administration	**Quantity**	**Percentage**
The American City & County	1	5.26%
Business Process Management Journal	2	10.53%
Journal of Public Administration Research & Theory	2	10.53%
Managing Service Quality	1	5.26%

Public Administration Review	4	21.05%
Total	**10**	**52.63%**
Information Systems		
Information Management & Computer Security	1	5.26%
Book	1	5.26%
ComputerWorld	1	5.26%
Communications of the ACM	3	15.79%
Information Systems Journal	2	10.53%
MIS Quarterly	1	5.26%
Total	**9**	**47.37%**

The literature search shows that there is an even distribution of publications in the business related disciplines as compared to the publications in information systems related outlets. The publication of e-government information in different disciplines suggests that the topic is multi-dimensional and is of interest to multiple research fields. It also illustrates the need to analyze a given phenomenon using the tools from different disciplines.

Recent reports on e-government initiatives show a growing trend among all levels of government. It is estimated that at the federal level only, the United States spent in excess of $2 billion in 2006 for e-government related activities (Belanger et al. 2006). Adoption of new technologies and strategies to enhance government activities in the online arena are present at virtually all levels of government. Publication of e-government research has occurred in both the public administration and information systems disciplines. Although most articles are broad in nature and typically deal with more theoretical and managerial implications of e-government, the literature review concluded in the following seven themes that were prevalent among extant e-government publications:

1. **e-Government Frameworks**: (Apostolou et al. 2011; Belanger et al. 2006; Chutimaskul et al. 2008; Cordella et al. 2010; Crichton et al. 2007; Dawes 2008; Gupta et al. 2003; Nour et al. 2008; Raus et al. 2010; Sarantis et al. 2011)
2. **Classifications of e-Government**: (Gupta et al. 2003; Layne et al. 2001; Zhou 2008)
3. **Types of services offered**: (Gil-Garcia et al. 2007; Gupta et al. 2003)
4. **Legislation concerning e-Government**: (Gil-Garcia et al. 2007; Taylor 2002)
5. **Common barriers to e-Government**: (Conklin 2007; Ebrahim et al. 2005)

6. **Citizens' trust and confidence in e-Government**: (Bélanger et al. 2008; Carter et al. 2005; Parent et al. 2005; Tolbert et al. 2003; Welch et al. 2005)
7. **Security concerns of e-Government solutions**: (Conklin et al. 2006; Kjaerland 2006; Wang 2009; Zhao et al. 2010)

The intricacy of e-government is described by some with a three stage model comprised of: initiation, infusion and customization. Yet others utilize another that focuses on communication as: one-way communication, two-way communication, exchanges and portals (Belanger et al. 2006).

Others when classifying e-government compare it to the more established discipline of e-commerce. When describing e-commerce transactions it is common to mention terms such as business-to-customer (B2C), business-to-business (B2B), business-to-employee (B2E) and customer-to-business (C2B). Similarly, e-government transactions can also be described in this same context as: government-to-citizen (G2C), government-to-employee (G2E) and government-to-government (G2G) (Moon et al. 2005). In this context, one can see that government can interact with citizens, employees, and even other governmental institutions in a comparative fashion as e-commerce (Carter et al. 2005).

Moon classifies e-government transactions into two distinct categories: financial and non-financial transactions (2005). Financial transactions typically include activities such as: paying for taxes, fines, licenses, utilities and citations. However, the larger list was comprised of non-financial transactions which included items such as: services requests, records requests/searches, maps, permit renewals, program registration and communication with elected officials. This evidence clearly demonstrates a trend in utilizing e-government for a growing number of services.

Information sharing among government agencies was a common theme prevalent among all levels of government. However, businesses utilizing e-commerce technologies were noted to typically shy away from information sharing as compared to the public sector (Caudle et al. 1991). However, one of the key deterrents in information sharing in governments agencies is a byproduct of incompatible legacy systems. The larger the agency the harder it becomes to stay current with technology and modernize legacy systems (Stamoulis et al. 2001). As such, e-government has also been implemented with the hopes of remedying this situation with the expectation that G2G transactions can be accomplished via such avenues despite more direct sharing methods.

Yet, despite the obvious advantages of e-government not only for citizen communication but also for intergovernmental transactions, many barriers still exist. Barriers can typically be classified into the following three categories: political, financial or technological (Ebrahim et al. 2005). Of particular interest are those that are technological in

nature. In some instances, there is no existing platform to perform a customized e-government service and developing such a service would be too cost prohibitive. Other limitations reside not with the governmental institution, but on occasion with a given community's demographics as it relates to their access to technology. Naturally, implementing a service that would have little or no usage would not be well advised.

Another common but frequently overlooked facet is a citizen's trust in a certain agency (Carter et al. 2005). Trust can implicate a given agency's reputation and past performance with the public. Or even more important, the lack of response from citizen initiated contacts from e-government services (Thomas et al. 2003). The perception that in-person contact will be more effective than online contact can have a devastating effect on a given e-government service. Research indicates that levels of trust in e-government are elevated with positive online responses and outcomes (West 2004). For that reason, government agencies should strive to ensure that online contact from citizens receives equal or greater support than contact from other traditional methods.

Of the various barriers mentioned, security seems to take a back seat (Norris & Moon, 2005). The paradox however, is that security is a growing concern amongst government agencies and their respective citizens (Taylor, 2002). Some agencies may just be too small to employ the necessary staff to address such issues, while others simply overlook the security concerns by highlighting the online service's features (Lee, Xin, & Trimi, 2005).

Larger agencies such as federal and state agencies typically provide for more thorough security measures because the likelihood of an attack is much greater. Unfortunately, many local government agencies fast-track security under the premise that such an investment is not necessary and therefore fail to implement proper security countermeasures. For this reason, many local cities and small government agencies have fallen victims to information breaches and other security threats. Research indicates that citizens are constantly becoming more "connected" by using computers, Internet, mobile phones and other forms of communication to stay in touch with their government agencies (Thomas & Streib, 2003). As such, a greater commitment to security is necessary from municipal government agencies.

One of the common barriers to implementing and adopting e-government solutions that was discussed earlier was "security". Public officials realize that e-government systems can place their entities at greater risk for terrorist or other malicious attacks (Halchin 2004). A recent security assessment on the state of e-government websites found the creation of opportunities and threats. The solutions provided a wide variety of services to citizens, but also created a myriad of new threats (Zhao et al. 2010).

Many methods exist to implement security for e-government. But in general e-government should address the three key areas of information security: confidentially, integrity and availability (McCumber 2005). Integrity can be conserved by ensuring that an audit trail is maintained and that all changes or updates to the systems are documented (van Velsen et al. 2009). Additionally, security should be a primary concern and needs to be built into the system and not performed as an afterthought once the system has already been fully developed (Meneklis et al. 2010). Lastly, risks should also be identified and evaluated to protect any citizen information that has been collected (Bélanger et al. 2008).

The literature review found a large pool of e-government related publications. However, the majority of the articles lacked a security focus. Part of the reason for this is that half of such articles were published in business, management or public administration journals. As such, the articles focused on managerial issues and strategies for implementation. Others discussed barriers for implementations and frameworks to describe and classify such e-government initiatives (Caudle 1990). The other half of publications were found in articles published in the information systems (IS) discipline. Unfortunately, even works published in IS conduits, failed to accurately address the need for security and especially at the municipal government level.

Security however, was not an unknown factor. Most articles touched on the topic of security, however not extensively enough to define a framework for addressing security implications of e-government. Instead, security was merely mentioned as a barrier or as a factor to consider when seeking to implement such a system (Moon et al. 2005). In many instances, security is often left last due to its intricate and complex application in the e-government arena. Although of extreme importance, management often seems to believe that security hurdles are the easiest to overcome (Mitrakas et al. 2007). For that reason, many initiatives often see delays. Security concerns are often not addressed and realized until the final steps of an implementation (Kaliontzoglou et al. 2005).

Based upon the findings, it is evident that more research is needed in this field. Researchers tend to focus on the larger federal and state agencies and often neglect the important role that local government plays in communities (Rice et al. 1982). As such, future research should seek to understand the limitations of smaller municipal government agencies to understand how they can still achieve and maintain a reasonable degree of e-government security.

CASE STUDY RESEARCH MODEL

This proposed research endeavor will utilize a case study research approach. The research will focus on understanding e-government within a municipal context to ascertain an improved understanding of how e-government is

influenced by this context (Myers 1997). As such this research study will adopt a set of philosophical assumptions that are inherent in interpretive research.

Case study research is an instrumental research model which is frequently used in information systems research (Orlikowski et al. 1991). This research will thereby adhered to the recommendations set forth by Walsham (1995) for interpretive case study research. Walsham prescribes a series of guidelines for interpretive studies to ensure that the role of the researchers is clearly defined. Following this set of recommendations ensures that generalizations can be formulated from the research findings.

RESEARCH METHODOLOGY AND DESIGN

Municipal e-government security will be analyzed as described earlier using a descriptive case study approach. Walsham (1995) supports an interpretive approach when conducting case study research "since it has been widely drawn on by organizational researchers concerned with interpreting the patterns of symbolic action that create and maintain a sense of organization".

For the case study design the recommendations set forth by Yin (2009) will be utilized. In designing a case study, Yin enumerates five key components of such a design:

1) Research Question(s)
2) Propositions (if any)
3) Unit(s) of Analysis
4) Logic Linking: Data to Propositions
5) Criteria for Interpreting Findings

Research Questions. Yin (2009) indicates that case study research is best suited to answer "how" and "why" questions. It is recognized that significant regulation is in place which requires federal agencies to comply with various security standards for their e-government solutions. The interest of this specific study is to take an in-depth look at e-government security practices for municipal government agencies using these three research questions.

1) What level of e-government security do municipalities currently have when benchmarked to federal e-government security requirements?

2) How can municipal agencies reach a federal level of e-government security?

3) Why are municipalities not fully compliant with federal e-government security requirements?

It is important to note that the first research question is not one that would typically be addressed by a case study research approach. However, this research question will be addressed as part of the study as it is necessary to baseline the current state of the municipalities that will be selected for this study.

Study Propositions. A principle component of this study focuses on the need to shed additional attention to and research on municipal e-government security. Earlier, it was identified that federal agencies have been provided ample regulation and also guidance for implementing security measures for their e-government initiatives. Due to the limited nature of extant research on municipal e-government security this study will take an exploratory approach. However, some propositions and assumptions will still be made.

- Proposition 1: The general lack of research interest and attention has caused many municipal government agencies to fall short on their security.
- Proposition 2: The gap in federal and municipal e-government security is a direct result of the lack of guidance and research coupled with limited resources for implementing such security.

Unit of Analysis. Identifying the actual component of what a "case" consists of can be challenging at times. However, defining a unit of analysis is a critical component of a case study research design. The point of analysis for this particular study is municipal government agencies. The case that will be analyzed is that of all municipalities within a large county within southern California. For purposes of anonymity the specific name of the county will not be revealed at this time. Additionally one key stakeholder will be selected from each agency to be interviewed.

Logic Linking: Data to Propositions. Two propositions were described earlier. The first proposes a general lack of interest in security for e-government agencies. The second purports that one of the reasons for which municipal government agencies struggle with security is because of their limited organizational resources and lack of security guidance. The study will encompass all the incorporated municipalities within a large county in southern California. The E-Government Security Act of 2002 requires federal agencies to provide security protocols to protect information. This requirement can be met by adhering to the guidelines of NIST Special Publication 800-44, Guidelines on Securing Public Web Servers. This publication

provides a series of 7 security checklists which a federal agency must follow to comply with the E-Government Security Act of 2002, 207(f)(1)(b)(iv).

As such, a comparative analysis of each organization to the NIST Publication 800-44 security checklists will be performed to: 1) initially baseline each municipality and 2) identify how agencies in general can become more compliant.

Criteria for Interpreting Findings. The findings of this case study will be closely correlated to each agency's compliance or lack thereof to the NIST 800-44 standard. Here an opportunity will be afforded to assess whether municipal government agencies can in fact comply with the federally required NIST 800-44 standard. It will also ensure that each organization is equally analyzed against a set of common criteria. The NIST 800-44 provides a series of 7 security checklists which can be used by an organization to gauge compliance with this standard. The degree of deviation or compliance with these security checklists will serve as the key basis for interpreting the findings of this study.

To provide a complete overview and picture of each of the municipalities, this high-level summary is provided to indicate the information that will be gathered from each agency. The case study will therefore include relevant information from each city such as follows:

Quantitative Data to Collect

- Name of Municipality
  - City demographics
- Financial Resources
  - Total City Budget
  - Total IT Budget
- Staffing Resources
  - Total city staff
  - Number of IT staff or contractors
    - Information security officer (if any)
    - Awareness of applicable standards from NIST, NSA or other applicable security standards
    - Information safeguards for e-government services
- Policies and Procedures
  - Collect any available IT security policy or procedures
- Security Baseline - NIST SP800-44 Survey
  - Checklist 1 - Planning and Managing Web Servers
  - Checklist 2 - Securing the Web Server Operating System
  - Checklist 3 - Securing the Web Server
  - Checklist 4 - Securing Web Content
  - Checklist 5 - Using Authentication and Encryption Technologies for Web Servers
  - Checklist 6 - Implementing a Secure Network Infrastructure
  - Checklist 7 - Administering the Web Server

A survey will be developed that assesses current compliance with NIST SP800-44 checklist standards. The survey will first ask each agency whether or not they are compliant with the listed security procedure. If the agency is not currently performing that security activity additional options will be presented to ascertain the ease to which that item can be attained.

Qualitative Information to Collect

To obtain a qualitative understanding of the nature of a given municipality an attempt will be made to speak to the key stake holder responsible for the oversight of information technology (IT) related operations. In most municipalities this typically consists of an IT manager or IT director. In instances, where a municipality utilizes solely contract IT staff, an effort will be made to interview the administrator or responsible party within the organization for managing that contact. In instances, where neither of these individuals is available, desired information will be obtained from the public relations office.

Interview Questions

1) What do you feel is the greatest challenge in implementing and maintaining e-government security for your agency?
2) What organizational change or resource would assist your agency in enhancing its e-government security?

EXPECTED RESEARCH CONTRIBUTIONS

Upon completion, this research will provide a substantial contribution to the e-government community in two facets: contribution to practice and a contribution to research and theory.

Contribution to Practice

This research project will provide contribution to the practice of e-government in two key areas as noted below.

Capacity – Provide a detailed analysis and review of the capacity to comply with federal security standards pertaining to e-government security and information privacy. The study will use the NIST SP800-44 document to baselines agencies and determine their level of compliance. Secondly, insight will also be provided to how agencies can become more compliant with this standard.

Resources – The research study will also provide a detailed overview of the technological resources and budget allocated for information systems. A specific focus will be made to identify the percentage of technology funds which are allocated for e-government services and related security mechanisms where possible. Table 2 shown below shows initial information that has been gathered from the 34 incorporated cities of Orange County, California. Each of these cities has a public facing website which is considered the first step towards e-government. All but one city were noted having e-government services. Additionally, the table provides information regarding the populations served by each city along with their adopted budget for the Fiscal Year 2011-2012. As the table shows, there is a variety in both city populations and budgets.

Table 2 – Orange County Cities with Population and Budgetary Information

City Name	Population (U.S. Census 2010)	Website	E-Government Services	Budget Fiscal Year 2011-12
Aliso Viejo	47,823	Yes	Yes	$ 13,440,955.00
Anaheim	336,265	Yes	Yes	$ 1,305,839,186.00
Brea	39,282	Yes	Yes	$ 84,671,801.00
Buena Park	80,530	Yes	Yes	$ 121,963,350.00
Costa Mesa	109,960	Yes	Yes	$ 94,650,182.00
Cypress	47,802	Yes	Yes	$ 33,129,770.00
Dana Point	33,351	Yes	Yes	$ 27,367,550.00
Fountain Valley	55,313	Yes	Yes	$ 33,863,160.00
Fullerton	135,161	Yes	Yes	$ 193,200,000.00
Garden Grove	170,883	Yes	Yes	$ 88,950,000.00
Huntington Beach	189,992	Yes	Yes	$ 183,547,977.00
Irvine	212,375	Yes	Yes	$ 136,206,801.00
Laguna Beach	60,239	Yes	Yes	$ 64,322,200.00
Laguna Hills	15,568	Yes	Yes	$ 35,650,191.00
Laguna Niguel	22,723	Yes	Yes	$ 41,043,398.00
Laguna Woods	30,344	Yes	Yes	$ 7,569,992.00
La Habra	62,979	Yes	Yes	$ 33,564,360.00
Lake Forest	16,192	Yes	Yes	$ 33,798,900.00
La Palma	77,264	Yes	Yes	$ 13,432,204.00
Los Alamitos	11,449	Yes	Yes	$ 15,629,823.00
Mission Viejo	93,305	Yes	Yes	$ 90,150,514.00
Newport Beach	85,186	Yes	Yes	$ 148,955,783.00
Orange	136,416	Yes	Yes	$ 170,949,929.00
Placentia	50,533	Yes	Yes	$ 57,654,595.00
Rancho Santa Margarita	47,853	Yes	Yes	$ 17,206,488.00
San Clemente	63,522	Yes	Yes	$ 114,343,420.00
San Juan Capistrano	34,593	Yes	Yes	$ 58,757,473.00
Santa Ana	324,528	Yes	Yes	$ 459,361,890.00
Seal Beach	24,168	Yes	Yes	$ 60,662,300.00
Stanton	38,186	Yes	Yes	$ 22,446,727.00
Tustin	75,540	Yes	Yes	$ 143,631,002.00
Villa Park	5,812	Yes	Yes	$ 3,934,000.00
Westminster	89,701	Yes	No	$ 127,712,077.00
Yorba Linda	64,234	Yes	Yes	$ 110,581,212.00

Contribution to Research and Theory

The primary output of this research project will be the development of a theoretical model which will address the three (3) key research questions surrounding municipal e-government security that have been posed by this paper. The theoretical model will answer the what, how and why of municipal e-government compliance to the NIST 800-44 standard.

This theoretical model will be used to establish a set of guidelines that can be generalized to any municipality desiring to reach compliance with the federal NIST 800-44 e-government security requirement. While it is anticipated that municipal agencies may not be able to comply with all aspects of federal security regulations for e-government, the guidelines will provide a series of recommendations to those which are most valuable and feasible. Focus will be placed on the ability to implement such procedures with a more limited set of resources as compared to the larger federal agencies.

RESEARCH AGENDA AND CONCLUSION

Although this case study is still underway, initial research and findings suggest that municipal agencies have significantly more limited resources as compared to larger federal and state agencies. These limitations frequently complicate the agency's ability to provide e-government security at par with federal agencies. This research also seeks to invoke further discussion within the e-government community to focus additional resources and future research on the specialized needs of municipal government agencies. This dialog is sought to increase the spotlight for improved security for e-government at the municipal level.

This paper provided an initial spotlight on municipal e-government security. It also provided the initial framework of an in progress case study focusing specifically on municipal e-government security. Additionally, it proposed three important research questions within this research context:

1) What level of e-government security do municipalities currently have when benchmarked to federal e-government security requirements?
2) How can municipal agencies reach a federal level of e-government security?
3) Why are municipalities not fully compliant with federal e-government security requirements?

However, many additional research avenues exist within municipal e-government security. The following topics are proposed for further research and exploration:

- Barriers and challenges in municipal e-government security.
- The importance of e-government security among stakeholders of municipal e-government initiatives.
- Development of a security model for municipal e-government initiatives.
- The cost of municipal e-government security breaches.

The increased use of e-government offerings at the municipal government levels coupled with the limited resources of such entities poses an important opportunity to focus on security. Initial research in this topic suggests that the extant knowledge base in municipal e-government security is virtually non-existent. Security however is becoming an increasingly notable theme in general e-government research and publications. As attention is focused on e-government security, research will need to include the intricacies of the lower levels of government that citizens most frequently interact with such as their local city, township or other municipality. By providing enhanced resources and research in this area, the e-government community can ensure that equal levels of attention are given to all levels of government and not just those with a larger presence such as federal or state entities.

REFERENCES

1. Apostolou, D., Mentzas, G., Stojanovic, L., Thoenssen, B., and Lobo, T. P. "A collaborative decision framework for managing changes in e-Government services," *Government Information Quarterly* (28:1), Jan 2011, pp 101-116.
2. Bélanger, F., and Carter, L. "Trust and risk in e-government adoption," *The Journal of Strategic Information Systems* (17:2) 2008, pp 165-176.
3. Belanger, F., and Hiller, J. S. "A framework for e-government: privacy implications," *Business Process Management Journal* (12) 2006, pp 48-60.
4. Carter, L., and Bélanger, F. "The utilization of e-government services: citizen trust, innovation and acceptance factors," *Information Systems Journal* (15:1) 2005, pp 5-25.
5. Caudle, S. L. "Managing Information Resources in State Government," *Public Administration Review* (50:5) 1990, pp 515-524.
6. Caudle, S. L., Gorr, W. L., and Newcomer, K. E. "Key Information Systems Management Issues for the Public Sector," *MIS Quarterly* (15:2) 1991, pp 171-188.
7. Chutimaskul, W., Funilkul, S., and Chongsuphajaisiddhi, V. "The quality framework of e-government development," in: *Proceedings of the 2nd International Conference on Theory and Practice of Electronic Governance*, ACM, Cairo, Egypt, 2008, pp. 105-109.
8. Conklin, A., and White, G. "e-Government and Cyber Security: The Role of Cyber Security Exercises,") 2006.
9. Conklin, W. "Barriers to Adoption of e-Government,") 2007.
10. Cordella, A., and Iannacci, F. "Information systems in the public sector: The e-Government enactment framework," *The Journal of Strategic Information Systems* (19:1) 2010, pp 52-66.
11. Crichton, C., Davies, J., Gibbons, J., Harris, S., and Shukla, A. "Semantic frameworks for e-government," in: *Proceedings of the 1st international conference on Theory and practice of electronic governance*, ACM, Macao, China, 2007, pp. 30-39.
12. Dawes, S. "An exploratory framework for future E-Government research investments," IEEE Computer Society, 2008, p. 201.
13. Ebrahim, Z., and Irani, Z. "E-government adoption: architecture and barriers," *Business Process Management Journal* (11:5) 2005.
14. Gil-Garcia, J. R., and Martinez-Moyano, I. J. "Understanding the evolution of e-government: The influence of systems of rules on public sector dynamics," *Government Information Quarterly* (24:2) 2007, pp 266-290.
15. Glaser, B. G., Strauss, A. L., and Strutzel, E. "The discovery of grounded theory; strategies for qualitative research," *Nursing Research* (17:4) 1968, p 364.
16. Gupta, M., and Jana, D. "E-government evaluation: A framework and case study," *Government Information Quarterly* (20:4) 2003, pp 365-387.
17. Halchin, L. E. "Electronic government: Government capability and terrorist resource," *Government Information Quarterly* (21:4) 2004, pp 406-419.
18. Hazlett, S.-A., and Hill., F. "E-government: the realities of using IT to transform the public sector," *Managing Service Quality* (13:6) 2003, pp 445-452.
19. Ho, A. T.-K. "Reinventing Local Governments and the E-Government Initiative," *Public Administration Review* (62:4) 2002, pp 434-444.
20. Kaliontzoglou, A., Sklavos, P., Karantjias, T., and Polemi, D. "A secure e-Government platform architecture for small to medium sized public organizations," *Electronic Commerce Research and Applications* (4:2) 2005, pp 174-186.
21. Kjaerland, M. "A taxonomy and comparison of computer security incidents from the commercial and government sectors," *Computers & Security* (25:7) 2006, pp 522-538.
22. Layne, K., and Lee, J. "Developing fully functional E-government: A four stage model," *Government Information Quarterly* (18:2) 2001, pp 122-136.
23. Marchionini, G., Samet, H., and Brandt, L. "Digital Government," *Communications of the ACM* (46:1) 2003, pp 24-27.
24. McCumber, J. *Assessing and managing security risk in IT systems: a structured methodology* Auerbach Publications, New York, 2005.
25. Meneklis, V., and Douligeris, C. "Bridging theory and practice in e-government: A set of guidelines for architectural design," *Government Information Quarterly* (27:1) 2010, pp 70-81.
26. Mitrakas, A., Hengeveld, P., Polemi, D., and Gamper, J. "Secure eGovernment Web Services," *Information Technology Newsletter* (18:1) 2007, p 21.
27. Moon, M. J., and Norris, D. F. "Does managerial orientation matter? The adoption of reinventing government and e-government at the municipal level," *Information Systems Journal* (15:1) 2005, pp 43-60.

28. Myers, M. "Qualitative research in information systems," *MIS Quarterly* (21:2) 1997, pp 241-242.
29. Nour, M. A., AbdelRahman, A. A., and Fadlalla, A. "A context-based integrative framework for e-government initiatives," *Government Information Quarterly* (25:3) 2008, pp 448-461.
30. Orlikowski, W., and Baroudi, J. "Studying information technology in organizations: Research approaches and assumptions," *Information Systems Research* (2:1) 1991, pp 1-28.
31. Parent, M., Vandebeek, C., and Gemino, A. "Building citizen trust through e-government," *Government Information Quarterly* (22:4) 2005, pp 720-736.
32. Raus, M., Liu, J., and Kipp, A. "Evaluating IT innovations in a business-to-government context: A framework and its applications," *Government Information Quarterly* (27:2) 2010, pp 122-133.
33. Rice, M. F., Alsobrook, R. A., and Weinberger, G. M. "Computer Security in Small Local Governments in Texas," *Texas Business Review* (56:2) 1982, p 100.
34. Sarantis, D., Charalabidis, Y., and Askounis, D. "A goal-driven management framework for electronic government transformation projects implementation," *Government Information Quarterly* (28:1), Jan 2011, pp 117-128.
35. Scherlis, W. L., and Eisenberg, J. "IT Research, Innovation, and E-Government," *Communications of the ACM* (46:1) 2003, pp 67-68.
36. Stamoulis, D., Gouscos, D., Georgiadis, P., and Martakos, D. "Revisiting public information management for effective e-government services," *Information Management & Computer Security* (9:4) 2001, pp 146-153.
37. Taylor, G. "Computer rules for network security," *The American City & County* (117:12) 2002.
38. Thomas, J. C., and Streib, G. "The New Face of Government: Citizen-Initiated Contacts in the Era of E-Government," *Journal of Public Administration Research & Theory* (13:1) 2003, p 83.
39. Tolbert, C., and Mossberger, K. "The effects of e-government on trust and confidence in government," in: *Proceedings of the 2003 annual national conference on Digital government research*, Digital Government Society of North America, Boston, MA, 2003, pp. 1-7.
40. van Velsen, L., van der Geest, T., ter Hedde, M., and Derks, W. "Requirements engineering for e-Government services: A citizen-centric approach and case study," *Government Information Quarterly* (26:3) 2009, pp 477-486.
41. Walsham, G. "Interpretive case studies in IS research: nature and method," *European Journal of information systems* (4:2) 1995, pp 74-81.
42. Wang, J. "E-government Security Management: Key Factors and Countermeasure," IEEE, 2009, pp. 483-486.
43. Welch, E. W., Hinnant, C. C., and Moon, M. J. "Linking citizen satisfaction with e-government and trust in government," *Journal of Public Administration Research & Theory* (15:3) 2005, p 371.
44. West, D. M. "E-Government and the Transformation of Service Delivery and Citizen Attitudes," *Public Administration Review* (64:1) 2004, pp 15-27.
45. Zhao, J. J., and Zhao, S. Y. "Opportunities and threats: A security assessment of state e-government websites," *Government Information Quarterly* (27:1) 2010, pp 49-56.
46. Zhou, P. "An Adaptive Framework for Managing Knowledge in E-Government," IEEE, 2008, pp. 69-73.