# Local Government Information Security Risk in the Age of E-Government

Eunjung Shin
Lauren N. Bowman
PhD Students

Eric Welch
Associate Professor

Department of Public Administration
Science, Technology and Environment Policy Lab
University of Illinois at Chicago

## Introduction

In an environment where citizens increasingly look to the internet for government information and services, information security remain key priorities for management and policy. Governments attempt to both serve and engage citizens, and to ensure citizen privacy by building secure online systems creates twin challenges of transparency and security, both of which affect the public's trust in government and the potential for the use of the internet for civic engagement. Addressing these challenges is particularly relevant as new technologies including cloud computing systems (Paquette et al. 2010) and interactive and social media functions become more widely available on government websites (PewInternet 2010). This dynamic is especially difficult to manage for local governments that have limited technical and financial resources to develop and maintain e-government systems.

To date, information security issues at the local government level have rarely been studied and it is difficult to determine how serious information security risks are for local governments. In order to devise relevant management strategies for secure but transparent e-government, it is necessary to first understand how serious the information security risks are, what information security measures already exist, and whether there are gaps in information security in local governments. This analysis provides an initial assessment of 1) the level of information security risk associated with local governments' e-government activities and 2) the potential organizational factors mediating information security risk (by comparing the level of the risk by organizational characteristics and policies). Using data from a 2010 national survey of local governments, this study shows what proportion of respondents have experienced online data breach attempts and actual accidental disclosures in the last two years. It also investigates how experiences with information security vary depending on organizational characteristics – organization size and department type– and organizational information security policy. We begin with a brief description of the data, proceed with a discussion of four findings, and finish with a summary and implications for local governments.

## Data

The analysis uses data from the web survey on e-government technology and civic engagement conducted by the Science, Technology and Environmental Policy Lab at the University of Illinois at Chicago and supported by the Institute for Policy and Civic Engagement. The survey was administered to government managers in 500 governments  with populations ranging from

25, 000 to 250,000. Because larger cities often have greater financial and technical capacity for e-government, all 184 cities with a population over 100,000 were selected while a proportionate random sample of 316 out of 1002 communities was drawn for smaller cities with populations under 100,000. For each city, lead managers were identified in each of five departments: general city management, community development, finance, parks and recreation and the police department. In total, 2,500 city managers were invited to take part in the survey. The survey was started on August, 2nd in 2010 and closed on XXX. A total of XXX responses were received for a final response rate of XXX. Some respondents chose not to answer the key information security questions in the survey resulting in a final sample size of XXX for this analysis. Because approximately XXX % of respondents chose not to respond to information security questions, these results may underestimate actual conditions in local governments.

**Finding 1: Moderate Information Security Risk Exists in Local Governments**

The analysis indicates a fairly substantial level of information security risk in local governments (Table 1). Department chiefs of local governments were asked if their organizations have experienced an attempted online security breach (e.g. hacking) during the last two years. Among all respondents, 13.4% reported having experienced an online data breach attempt. An additional 40% of all respondents chose "don't know", which may indicate either a lack of awareness of information security issues or a lack of occurrence of information security-related events. Second, respondents were asked whether their local government had experienced any unexpected electronic information disclosure during the last two years. For this question, 7.7% of respondents indicated "yes" and almost 20% of them provided "don't know" responses. This indicates that while local governments are subject to accidental information disclosure via the Internet, the problem is moderate rather than severe. Overall, affirmative and "don't know" reports of data breach attempts are approximately two times higher than unexpected disclosure events. This probably indicates that the relative risk of disclosure from external threats is a critical facet of local government management of electronic data.

Table 1. Information Security Risk in U.S. Local Governments in the Last Two Years

| **Online Data Breach Attempts** | | | **Unexpected Electronic Information Disclosure** | | |
|---|---|---|---|---|---|
| Yes | 102 | (13.4 %) | Yes | 59 | (7.7 %) |
| No | 354 | (46.5 %) | No | 552 | (72.4 %) |
| Don't Know | 306 | (40.1 %) | Don't Know | 151 | (19.8%) |
| Total | 762 | (100.0%) | Total | 762 | (100.0%) |

**Finding 2: Large Governments Report a Higher Level of Information Security Risk**

The level of information security risk differs depending on the size of local government. Large local governments with financial resources higher than the median total budget for all local governments ($13,000,000) are more likely to report that external actors have tried to access to their electronic data without proper authorization (Figure 1). Among respondents from large governments, 16% indicate they have experienced an attempted breach. This compares to 12%, of small governments who indicated the same experience. In addition, large governments are more likely to say that they have experienced unexpected electronic information disclosures compared to small governments (Figure 2); 9% of large government and 6% of small governments respondents admit they had an unexpected disclosure experience.

The difference between small and large organizations requires further examination because respondents from small organizations, due to lower resources, may not be aware of information security issues. Concerns about the low level of awareness in small governments is supported by the finding that small local governments are more likely to indicate "don't know" about information security issues compared to large local governments. The proportion of respondents in small governments (46.9%) indicating "don't know" about data breach attempts is considerably higher than that of large governments (31.4%). Hence, information security risk in small local governments might be underestimated due to the lower level of awareness about the information security issue.

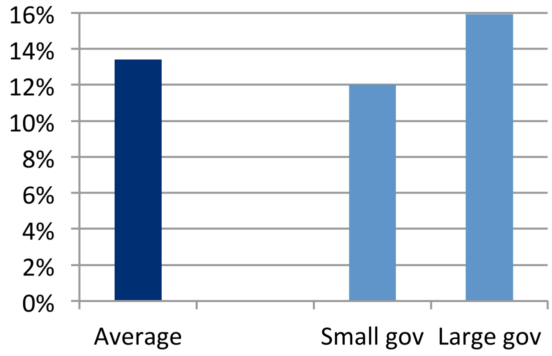

Figure 1. Online Data Breach Attempts

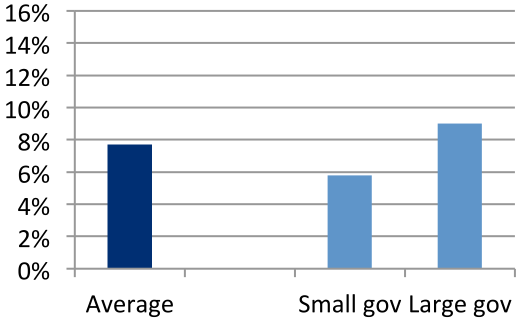

Figure 2. Unexpected Information Disclosure

**Finding 3: Information Security Risk Varies across Departments within a Government**

Level of reported information security risk also varies by local government department (Figures 3 and 4). City managers and chief finance officers are more likely to say that their organizations have experienced an attempted security breach, while police departments are less likely to report both data breach attempts, as compared to the average for all respondents. Community development respondents report lower than average attempted breaches, while police and parks and recreation report approximately average levels.

When it comes to unexpected information disclosure, three departments – city managers, community development and parks and recreation – report higher levels of risk than the average. This finding may have implications for public engagement activities because these departments often engage with citizens in decision-making processes. To secure information and maintain trust of citizens, greater emphasis on infomraiton security risk reduction in these departments may be necessary. Overall, the variation in breaches and disclosures across departments indicates the potential for cross-department learning and information exchange to reduce information security risk.

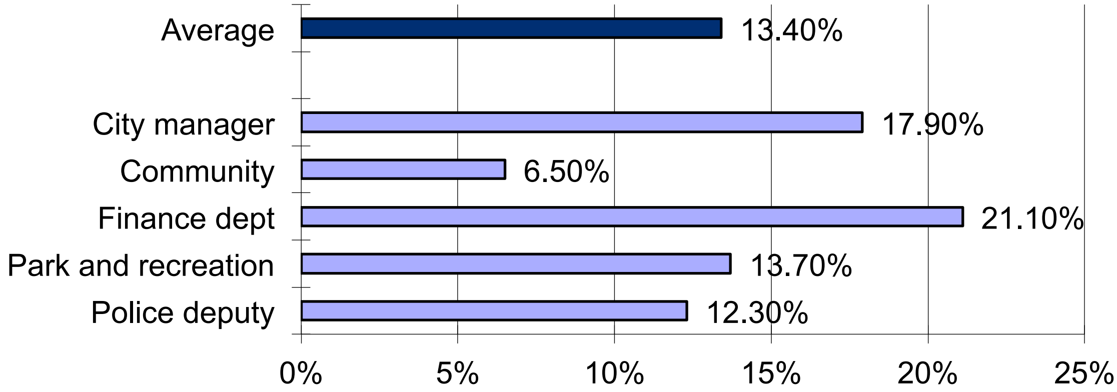

Figure 3. Local governments experiencing online data breach attempts I

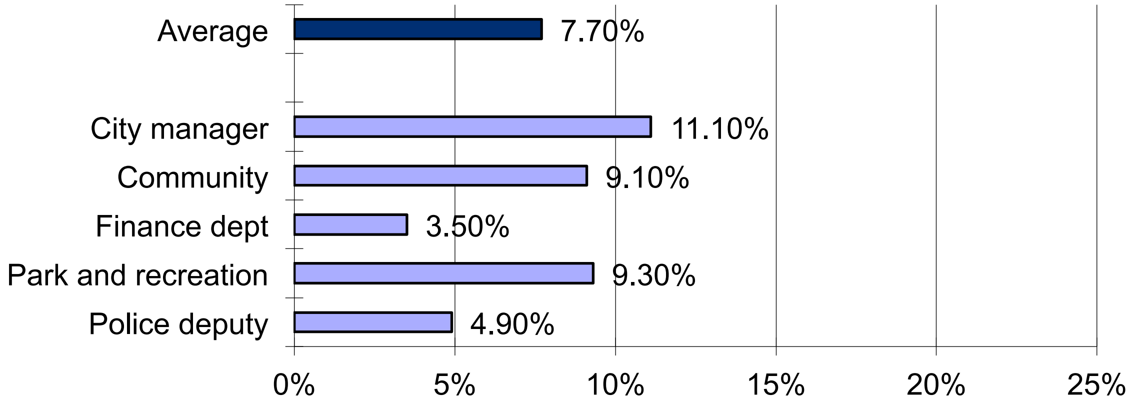

Figure 4. Local governments experiencing unexpected electronic information disclosure

**Finding 4: Information Security Policy Awareness is Associated with Information Breach**

Information security policies are implemented in order to prevent the accidental release of sensitive information and outside access to data and documents. The local governments that took part in the survey recognize the necessity of security measures, with a majority of respondents reporting that they have information security policies: 79 % of respondents either strongly agree or agree with the statement that their organizations have adopted clear policies to ensure security of their documents and data.

The presence of information security policies may moderate the level of information security. A Chi-square test ( $\chi^2$=9.03, df=4, p-value=0.06) shows that there exists statistical difference in data breach attempts among the three groups: 1) respondents whose organizations have clear security policies, 2) respondents that do not have clear security policies, and 3) respondents that are not sure about their security policies. As Table 2 illustrates, respondents that indicate their organization does not have security policies are more likely to report experiencing an attempted breach of data online. This probably indicates that government organizations are responding to these threats and are seeking to reduce information security risk. The large percentage of respondents who fall into the "Don't Know" category raises questions about the perception of information security by those within local governments. It is possible that there is limited communication between information departments or employees, and other departments or employees. Alternatively, respondents may be hesitant to admit that their organization does not have security policies or that they had experienced security problems. These issues will require further investigation in the future.

Table 2. Online Data Breach Attempts and Security Policy

| | | Local Government Information Security Policy | | |
|---|---|---|---|---|
| | | With policy | Without policy | Unsure about policy |
| Online Data Breach Attempts | Yes | 84 | 7 | 11 |
| | | (14.0%) | (6.6%) | (20.4%) |
| | No | 278 | 47 | 26 |
| | | (46.4%) | (44.3%) | (48.1%) |
| | Don’t Know | 237 | 52 | 17 |
| | | (39.6%) | (49.1%) | (31.5%) |

## Summary and Implications for Local Governments

This analysis investigated the level of online information security risk in local governments and potential factors related to the occurrence of breaches and disclosures. The analysis found that 13.4% of respondents report a data breach attempt and more than 7.7 % of them report unexpected information disclosure via the Internet. While this appears to be a relatively moderate level of information security risk, there is substantial variation in these findings across local government departments.

Organizational factors associated with the level of information security risk are also identified. Government size, in terms of a total amount of budget, and department characteristics are two factors affecting perceptions and reporting of information security policies and issues. Local government security policies themselves are another indicator of data breach attempts. Additionally, the large percentage of “Don’t Know” responses across all questions may reflect a potential risk caused by general lack of awareness of security issues as well as possible unreported risk. This highlights a potential need for increased awareness of security issues organization wide, not just in those departments where security is an immediate concern. Without additional and ongoing attention to information security risk, local governments may undermine their attempts to more gain citizens’ confidence and to more fully engage them through the use of electronic media. Overall, this analysis calls for more comprehensive research to understand organizational and individual factors associated with the level of information security risk in the process of developing and maintaining e-government systems.

## References

PewInternet. (2010). Attitudes towards Online Government Services. Government Online. retrieved from http://www.pewinternet.org/Reports/2010/Government-Online/Part-Three/Attitudes-towards-social-media.aspx?r=1 (September, 10, 2010).

Paquette, S., Jaeger, P.T. and Wilson, S.C. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly* 27(3), 245-253.

*Questions about this research should be directed to Mary K. Feeney, PhD, Associate Professor, UIC Department of Public Administration - mkfeeney@uic.edu*