Chapter 6
Local Government Homeland Security Information Systems

INTRODUCTION

This chapter examines homeland security information systems (HSIS) with a focus on local governments. Local governments are typically the first at the scene when responding to an emergency or a terrorist attack. The most notable incidents are Hurricane Katrina and the terrorist attacks of September 11, 2001. In both of these incidents the first responders were the local governments, which faced dual issues of communication and information sharing. It is important to understand the current level of preparedness and use of HSIS in local governments. This chapter tries to discern the relative priority of HSIS compared to other priorities of local governments in the realm of homeland security.

This chapter first outlines some background information on local governments with respect to their organizational structure and level of homeland security preparedness. The second section outlines the stages of e-government adoption, which is commonly discussed in the local e-government literature. Third, there is a discussion of homeland security information sharing between the federal, state, and local governments. There is some evidence presented from existing surveys of the impact of HSIS on local governments. Finally, there is survey results presented from a study conducted by the International City/County Management Association (ICMA) on homeland security preparedness. This survey information is used to determine where HSIS fits into local priorities on homeland security.

BACKGROUND ON LOCAL GOVERNMENTS

The federal government has strong incentives for disaster management and preparedness; local governments often lack the administrative capacity or commitment for effective policies (Gerber, Cohen, and

DOI: 10.4018/978-1-60566-834-5.ch006
Stewart, 2007). The federal system because of its conflicting incentives, lack of management coordination, and uneven resources has a difficult time providing comprehensive disaster preparedness. Local governments because they are first on the scene provide a key role in homeland security.

When examining local government HSIS, it is important to understand the type of government. The two main forms of government that cities have adopted are the council manager and mayor council structures (DeSantis and Renner, 2002). Proponents of the council-manager form of government argue that this structure centralizes administrative responsibility in the hands of one individual, normally called the city manager. However, the distinction between the different forms of government have been blurred with for example the major-council governments increasingly hiring a Chief Administrative Officer (CAO) who performs similar tasks as the city manager. In addition, many council manager governments have strengthened the role of the mayor. The literature on e-government adoption in local governments generally has found that council-manager governments have been greater innovators of e-government diffusion than other forms of government. This is attributed to the professional city manager wanting to use e-government as a way of strengthening reforms within the city.

Research results indicate that cities that are more innovate in management culture are more receptive to the adoption and advancement of e-government (Moon and Norris, 2005). The reasoning is that more innovative governments tend to be more receptive to new managerial and technical approach such as e-government. These cities tend to adopt change better because there is less administrative resistance. Governments that are strong adopters of information technology, such as e-government, should also have a capacity to use HSIS as well.

In a review of a future research agendas for counties two areas of 15 identified by Streib, Svara, and Waugh, et. al. (2007) was homeland security and IT related. With respect to the former many counties have many other pressing issues on their agenda and homeland security must be included with this. For example, as noted later in this chapter many counties do not take the threat level indicated in the homeland security advisory system very seriously, and do not increase security when the threat level rises. The second issue of IT indicates that there is optimism that IT could potentially solve many of the service issues that have plagued counties, but the greater issue is pay back, if a system is build will there be a return on investment. There are additional issues of privacy of data collected by counties and what will become of the information.

Clarke and Chenoweth (2006) make the argument that terrorism is a city-specific activity. They believe that there is a potential for non-metropolitan areas to be a terrorist target, to date terrorist attacks on the U.S. have been an urban occurrence. Cities are center of power, the focus of media, and complex enough to hide terrorist activities. Cities are tightly coupled systems which makes them especially prone to risk of a terrorist attack.

An interesting case study of IT planning for the Year 2000 (Y2K) problem in Iowa cities and counties revealed that many local governments did not have concrete plans to handle the problem of Y2K (Ho and Smith, 2001). This lack of planning was influenced mostly by the attitude of senior management toward the Y2K problem. Essentially, their results indicate that IT planning depends on the attitude of senior management towards the problem. The more concerned senior management is, the more likely that they will participate in IT planning.