Information Portal Strategy for Transportation Security Management

Ying Wang
University of Texas-Pan American, USA

INTRODUCTION

Tokyo subway poison gas attack in 1995, the infamous September 11 in 2001, Madrid train bombings in 2004, London bombings in 2005, "underwear bomber" in 2009: the series of attacks on air-borne and surface vehicles by terrorists have awakened the global awareness on transportation security. Transportation systems, due to their huge passenger and goods volumes, relatively easy access and diversity in ownership and management, have become the primary targets of terrorists in the era of mass terrorism (Leung, Lambert & Mosenthal, 2004; Johnston, 2004; OHS, 2002). The injury and damage of such attacks are often catastrophic with far-reaching impacts on public psychology. In addition to the death toll of thousands, GAO (2002) reported that the attacks on the two World Trade Center buildings cost about $83 billion in total losses (including both direct and indirect costs). Psychologically, 44% of the adults reported one or more substantial symptoms of stress, and 90% had one or more symptoms to at least some degree (Schuster et al., 2001). It is not a question whether there will be another major terrorist attack on the transportation systems, but when and where. Thus, enhancing transportation security is a critical part of the war against the terrorism.

The federal government (OHS, 2002) defines homeland security as "a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur" (p. 20). Derived from it, transportation security management can be defined as the concerted effort to prevent terrorist attacks on, reduce the vulnerability of, minimize the damage and recover from attacks that do occur to transportation systems. In other words, transportation security management requires the coordination and cooperation among key players.

One critical component of effective transportation security management is information sharing among key players through information technology (Clemons & Row, 1992). Information technology (IT) has been well-recognized as an important tool for transportation security (Kaza et al., 2009). However, better technology does not necessarily mean better security, as evidenced by the decline of airport security in the last decade of the twenty century (GAO, 2001). The hijackings of September 11 exposed the flawed arrangement and mismanagement of security systems (Seidenstat, 2004). To materialize the full potential of technology, a strategy regarding how to use IT to involve all key players in the coordinated effort is needed. However, little discussion has been made on such an IT strategy in transportation security management.

IT strategy is related to how to apply information technology for a strategic purpose, and it incorporates the range of issues from strategy formation to system implementation (Galliers, 1993). In organizational settings, the optimal IT strategy is to achieve business competence through business process reengineering that is driven by both business goals and technological advances (Galliers, 1994). Through reengineering the security processes in a similar way, a well-developed IT strategy may enhance transportation security management.

BACKGROUND

Before 9/11, transportation security is mostly the responsibility of airlines, railroads, subway systems, and other mass transit systems (Waugh, 2004). These public transport providers can be generally referred to as the "carrier" in transportation security management as they take charge of both the facilities (e.g. air/seaports, railway/bus stations) and the vehicles (e.g. airplanes, ships, trains, buses) of different transportation modes.

DOI: 10.4018/978-1-4666-5888-2.ch425

After 9/11, the government intervened much more extensively. For instance, the Transportation Security Administration took over a significant proportion of security responsibilities, such as passenger and baggage screening, from the carrier side (Frederickson & LaPorte, 2002). The government also supports the carrier to enhance transportation security in form of federal grants through agencies such as Federal Aviation Administration (GAO, 2007; Moynihan & Roberts, 2003). The "government" here in transportation security management, in a broader sense, includes federal and state agencies at different levels and their connections with foreign governments and international organizations.

The dominance of federal government in security management has enhanced transportation security, but it leads to other issues. First of all, terrorist attacks are hard to predict but require quick responses, demanding numerous entities at different levels in both the public and private sectors to cooperate and coordinate closely with each other (Johnston, 2004; Wise & Nader, 2002). Such collaborations need the close coupling of terrorism preparedness, crisis management and consequence management (Wise & Nader, 2002). Also, the social, economic and fiscal dislocation imposed by terrorist attacks is beyond the capability of government alone (Posner 2002, p. 4). In allocating federal funding to enhance security, the government has been criticized for the lack of transparency and efficiency (Mayer & Carafano, 2007). For example, the Department of Homeland Security allocates $765 to improve security in urban areas (including transportation facilities) in the year of 2006, but the criteria for allocating such grants are not very clear and there are questions about such practices (Liberman, 2006).

One thing that the current mode of transportation security management lacks is the full consideration of the public in terms of their rights and responsibilities in transportation security management (Abeyratne, 2010). In transportations security, the public includes the passengers and general public. In addition to other tangible and intangible resources, the public has the legitimate rights and needs to access relevant security information, and may even provide critical security information. For example, it was the owner of the SUV hijacked by 2013 Boston Marathon bombers who reported the personal encounter, and his cellphone left on the vehicle allowed the police to track the terrorists (Harris, 2013). The involvement of the public also helped the authority identify the suspects quickly once the surveillance-camera images were posted on Facebook and other social networks (Smith & Patterson, 2013). Thus, the public needs to be included as one of the key players along with government and carrier in transportation security management. Accordingly, the optimal IT strategy must enable all of them to share information with each other and concert the effort effectively against potential terrorist attacks.

MAIN FOCUS OF THE ARTICLE

Statement of Objectives

The appropriate IT strategy should be based on the understanding of how IT can be used to facilitate government, carrier, and public to carry out different aspects of transportation security management in a more effective way. Though there have been abundant discussions on organizational IT strategy, few discussions have been made on the IT strategy related to security management. In the management literature, the most relevant theory is the stakeholder theory. In his landmark work "Strategic management: A stakeholder approach," Freeman (1984) proposed the use of stakeholder analysis for the guidance of strategy making. Therefore, the first objective of this article is to conduct a stakeholder analysis on the transportation security management to identify the stakeholders and their interests, roles and relationships with each other. Based on the analysis, the next objective of this article is to find out the optimal IT strategy to involve all stakeholders in transportation security management.

This article identifies the government, carrier and public as the stakeholders in transportation security management. Based on the discussion of their interests, roles and relationships, it explores the use of information portal approach as the IT strategy that allows all stakeholders to share information with each other. Information portals have been widely used in corporate settings as the primary methods to organize and discover corporate resources (Orenstein, 1999). This article will extend the information portal approach to transportation security management for the purpose of enabling all three stakeholders to participate in its different processes, including security assessment, security control and security communication.