

# Security in E-Government: Two Binary Models and a Framework

Dr. Richard A. McMahon  
University of Houston-Downtown  
[McMahonR@uhd.edu](mailto:McMahonR@uhd.edu)

## Abstract

This work presents two models and a design framework developed for the study of e-government security. These models and the framework were created in an effort to help fill the gap reported in the literature regarding a lack of e-government models. They also serve as a connection between security in the relatively new field of e-government and a larger universal concept of general security dimensions. The two models were created so that security implementations could be depicted in a binary format so that an e-government design framework could be developed. The initial indications from employing this design framework provide researchers with qualitative justification for further inquiry and suggest increased benefits from applying further refinement to the framework's implementation.

## Introduction

A model can be defined as a replica of complex phenomena, typically creating a graphic representation (Isaac & Michael, 1995). Heeks and Bailur (2006) indicated very little use of models in e-government research and implored future researchers incorporate more modeling in their studies. This present study included the development and use of two such models in order to facilitate creation of a design framework. These models and the design framework will also help fill the gap in model use within e-government research in the same fashion as the e-government maturity model put forth by Booz Allen Hamilton, Inc. (2001a; 2001b). In research, models may be equated to theories when major components of the model represent relationships between constructs (or concepts). Constructs were seen as “nonobservable hypothesized characteristic[s] ... inferred to be present ... on the basis of a linkage of observed events or activities” (p. 2). Circles, squares, or rectangles frequently reflected constructs with arrows joining them to indicate impact or interaction between constructs.

In one of his early approaches to describing e-government, this time clarifying a single aspect of the broader overall concept, Relyea (2001, 2002), while documenting e-government's development, discussed several of what he called general dimensions applicable to electronic government security. These general e-government-applicable security dimensions were then envisioned for their interactive nature as components within a wider perception of security, described as encompassing four protective dimensions (McMahon, 2003b).

While incorporated in this work's security models and its e-government security design framework, the four protective dimensions were actually considered to be applicable to any system's security, including the business-like environment in which e-

government can be included. Furthermore, correspondence with the author initially envisioning the possibility of general security dimensions (Relyea, 2001, 2002) indicated agreement (H. Relyea, personal communication, April 11, 2005) with the following two models' portrayal of his general dimensions within this work's four protective dimensions.

### Threat Structural Dimension Model

This work's first model, shown in Figure 1, presents the researcher's graphical representation of an increasingly heightened threat dimension with its corresponding need for an increasing security presence in the form of an expanding structural dimension. Starting on the left of the model, it can be seen that if there was no threat, there would be no requirement for an increase to the system's structural dimension. The answers to the questions in the white boxes between the model's dimensional arrows would indicate the increasingly complex structural requirements of the e-government presence facing the threat rising against it.

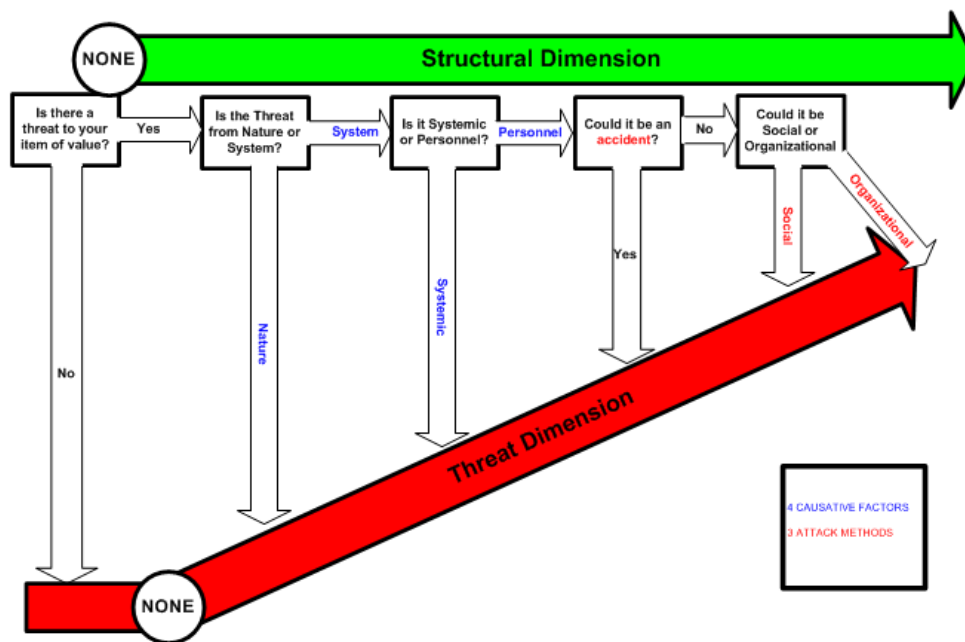


Figure 1. Security model - threat and structural dimension.

The structural dimension in the model depicted as the green arrow in Figure 1 shows one of the four protective dimensions, discussed in the following section, that were envisioned by McMahon (2003b) as incorporating Relyea's (2001, 2002) general view of security dimensions in conjunction with the four causative factors and three attack methods associated with security threats (McMahon, 2003a). The model also represents an easily interpreted security depiction for subsequent computer modeling because of its

principal use of binary (e.g., yes/no, either/or) type statements. This binary security depiction was also incorporated within the e-government framework discussed below.

### Threat Protective Dimensions Model

This work's second model, shown in Figure 2, presents the researcher's model to graphically represent the interactional response requirements from a security system's four protective dimensions (green arrows) as the increasing threat dimension (red arrow) forces change within the system. The dichotomous responses to questions posed in the white boxes, intertwined between the five dimensions depicted in Figure 2, can be seen as beginning at the left with no protective dimensional requirements, no threat dimension, and no item to protect. The binary-type responses to the questions in those white boxes would take the security system implementer through security's two truisms, its two basic concepts, two types of loss, two types of objects, four kinds of data, four kinds of services, and four threat outcomes (McMahon, 2003a) as the rising threat would thus create the need for increases in each of security's four protective dimensions.

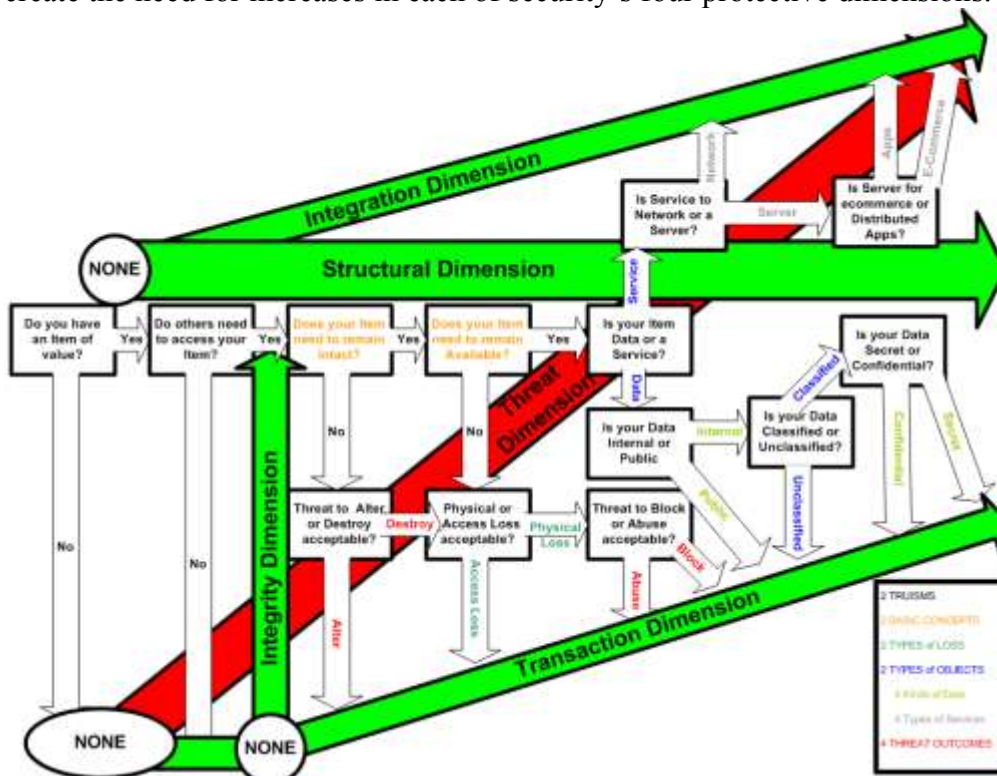


Figure 2. Security model - threat and four protective dimensions.

### Result: E-government Design Framework

The security models provided in Figures 1 and 2 were used to develop a framework of e-government security. The framework linked the models' four protective dimensions to the four stages or phases of an e-government model (e.g., Miranda, 2000; Symond, 2000). Similarly, the Booz Allen Hamilton e-government maturity model (2001a; 2001b) included four *levels* of an organization's e-government development. Much like the

framework constructed by Heeks and Bailur (2006), this researcher's framework development was multi-dimensional. Although Heeks and Bailur used two dimensional continua, each depicting perspectives from optimism to pessimism relative to each of the two dimensions being reported about differing views of the government, the framework of this work was three dimensional. This researcher, however, incorporated a simpler binary (e.g., yes/no; male/female) system for coding responses into its framework rather than using continua.

The result of answering the binary-type questions while utilizing a coding instrument to facilitate interpretation of this researcher's content analysis was the two by two by two e-government design framework matrix depicted in Figure 3. Further, the matrix was related to the literature's typically discussed (Heeks & Bailur, 2006) phases and stages (e.g., Miranda, 2000; Symond, 2000) or levels (Booz Allen Hamilton, Inc., 2001a; 2001b) of an e-government implementation.

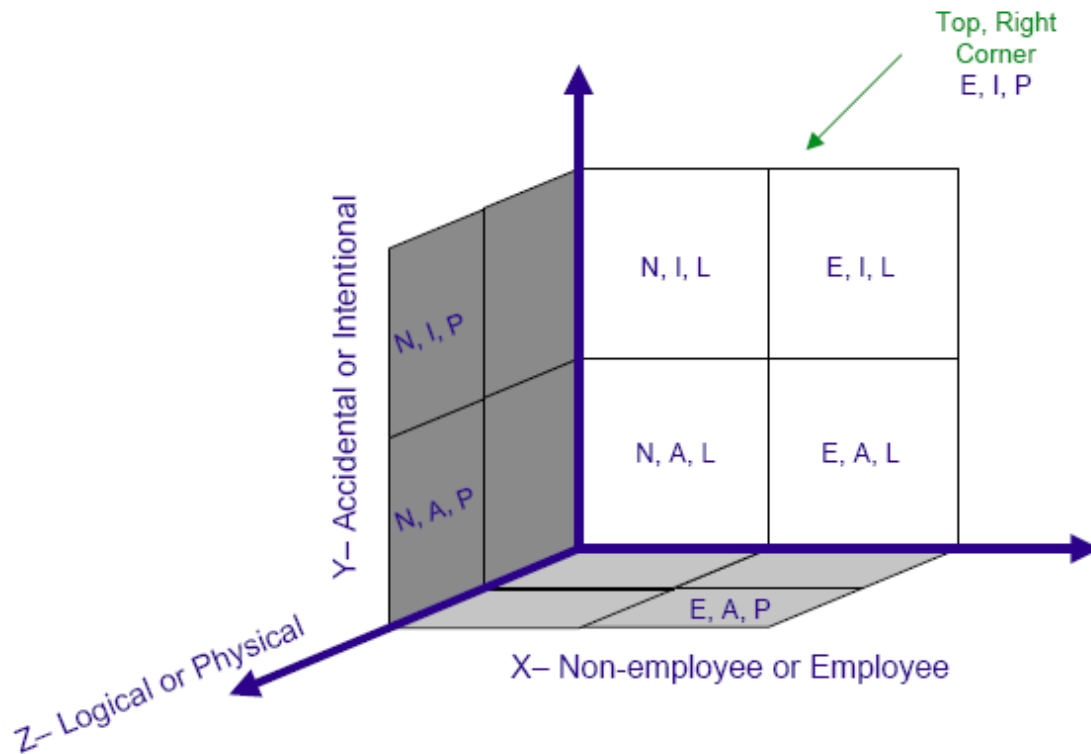


Figure 3. E-government security threat design framework matrix.

## References

- Booz Allen Hamilton, Inc. (2001a). *E-Government Maturity Model: From Assessment to Action*, July. Retrieved September 10, 2010, from [http://www.boozallen.com/consulting/industries\\_article/658788](http://www.boozallen.com/consulting/industries_article/658788)
- Booz Allen Hamilton, Inc. (2001b). *E-Government Maturity Mode*, July. Retrieved September 10, 2010, from [http://www.boozallen.com/media/file/e-gov\\_model.jpg](http://www.boozallen.com/media/file/e-gov_model.jpg)
- Heeks, R. & Bailur, S. (2006). *Analysing eGovernment research: Perspectives, philosophies, theories, methods and practice*, (iGovernment Working Paper No. 16), University of Manchester, UK: IDPM. Retrieved September 10, 2010, from <http://www.sed.manchester.ac.uk/idpm/research/publications/wp/igov/documents/iGWkPpr16.pdf>
- Isaac, S. & Michael, S. (1995). *Handbook in research and evaluation: For education and the behavioral sciences* (3rd ed.). San Diego, CA: Educational and Institute Testing Services.
- McMahon, R. (2003a). *Netability series: Security design: Microsoft Windows 2000*. St. Paul, MN: EMC/Paradigm Publishing.
- McMahon, R. (2003b). *Perspectives of e-government: From the watchful eyes of security*. Proceedings of the 13<sup>th</sup> Association for Chinese Management Educators International Conference on Pacific Rim management. Seattle, WA: July 31 - August 2.
- McMahon, R. (2007c). *Electronic Government: Development of a Design Framework*. Unpublished doctoral dissertation, Argosy University, Sarasota, Florida.
- Miranda, R. (2000). The building blocks of a digital government strategy. *Government Finance Review*, 16(5), 9-13. Retrieved April 15, 2010, from Wilson Web database.
- Relyea, H. (2001). E-gov: The federal overview. *The Journal of Academic Leadership*, 27(2), 131-148. Retrieved January 27, 2009, from Wilson Web database.
- Relyea, H. (2002). E-gov: Introduction and overview. *Government Information Quarterly*, 19(1), 9-35. Retrieved January 27, 2009, from Wilson Web database.
- Symond, M. (2000, June 24). Government and the Internet: No gain without pain. *The Economist*, 355, 9-14. Retrieved June 17, 2010, from EBSCO database.