Computer Security in Electronic Government: A State-Local Education Information System

Alison Radl, Iowa State University, USA
Yu-Che Chen, Iowa State University, USA

ABSTRACT

As e-government projects proliferate at all levels of government, and as they transition from voluntary to mandatory participation, close examination is required, particularly the examination of security issues. The CIA (Confidentiality, Integrity, Availability) model offers a framework for examining e-government projects. This study examines the factors impacting security, using as a case study an education information system in the 2003-2004 school year. The study focuses on how CIA factors relate to a host of variables, such as school district size, software selection, technology staffing, technical competence and support, awareness of security issues, and project commitment. For the organizations participating in the project, typical factors of district size and software selection are found to be insignificant, and technical support is identified as one of the key factors promoting security.

Keywords: IS evaluation; IS security; IT in public administration

INTRODUCTION

E-government refers to the use of information and communication technology to carry out government operations such as delivering government information and services. E-government has grown in the past decade. E-government efforts can vary from Web portals to online license renewals to experimentation with online voting. E-government is generally recognized as a means of making government more efficient while allowing it to be more responsive to customer needs. The growth in e-government has been rapid. For example, in the United States, the percentage of local governments with Web sites increased from 8.7% in 1995 to over 80.0% in 2000 (Holden et al., 2003). Advances in information and communication technology are helping to make the growth in e-government a global phenomenon. A United Nations report shows that governments around the world are moving towards higher levels of e-government to better serve their citizens (UN-ASPA, 2002).

For the evaluation of e-government projects, there are a number of approaches grounded in the information systems research literature. One method calls for ex-
amining e-government projects in terms of the factors promoting implementation (Brown et al., 1998; DeLone, 2003; King et al, 1994; Shaw, 2003). Adoption and user-acceptance constitute another approach (Brown, 2003; Davis, 1989; Ho & Ni, 2004; Venkatesh & Davis, 2000). Some scholars focus on various aspects of administrative reform, focusing on impacts on efficiency, transparency, and accountability arising from the use of information and communication technology (Brown & Brudney, 1998; Danziger & Andersen, 2002; Ho, 2002; Moon, 2002; Pandey & Bretschneider, 1997; West, 2004).

Moreover, a wealth of studies on e-government initiatives around the world offers opportunities for comparative understanding. The United Nations has issued a report consisting of a comprehensive country-by-country account of e-government activities. The report offers advice on building institutional foundations for continuing success (UN-ASPA, 2002). The Cyberspace Policy Research Group examines the transparency, democratization, and accountability of e-government projects. Since 1995, it has examined national government Web sites around the world. Working with scholars and practitioners around the world, Heeks (2001) has proposed a generic framework for developing and implementing e-government projects. He offers detailed country- and project-specific case studies.

And yet among the current studies of e-government, a common theme recurs: Despite the increasing need for such research, there is a lack of comprehensive evaluations of information and computer security. Comprehensive evaluation involves assessing the confidentiality, integrity, and availability of the information under government control. While several studies have attempted to examine computer security issues (Ives et al., 2004; Karr et al., 2003; Pierce, 2004), they have focused only on a single aspect of computer security.

Two concurrent trends underlie the need to evaluate the security of e-government projects. First, a growing amount of confidential citizen data is being gathered through e-government projects. One prominent example in Europe is the modernization of National Health Services in England. The data spine of this e-government project will have all critical medical information of every citizen in the country. Online tax filing and employment applications are also examples of e-government initiatives that collect personal and financial information. The increase in the collection of confidential data arises in part due to the transition from voluntary to mandatory participation and requirements that lower-level governments submit electronic data to higher-level governmental offices. Second, increasing cyber-crime activities poses greater risks for e-government information systems. Statistics from the Carnegie Mellon CERT Center indicate an approximately 13-fold increase in security incidents from 1999 to 2003. Such identified widespread weaknesses pose a threat to government information systems (US General Accounting Office, 2000). As more and more government and commercial activities take place online, nations around the world grow increasingly concerned about cyber-security.

There are two main reasons why this study focuses on an education information system that requires vertical integration of government operations. First, education is one of the prominent government service areas amenable to computer security studies. Compromises in the security of confidential student information can result in dire consequences for students and their families. The reach of the education informa-
Related Content

City E-Government: Scope and its Realization
Hanuv Jit Singh Mann, Gerald Grant and Inder Mann (2013). E-Government Services Design, Adoption, and Evaluation (pp. 39-52).
www.igi-global.com/chapter/city-government-scope-its-realization/73033?camid=4v1a

Social Inclusion and OmbudsOffice Websites in Canada
www.igi-global.com/chapter/social-inclusion-and-ombudsoffice-websites-in-canada/110316?camid=4v1a
Web 2.0, ICT Infrastructure, and Training Provision for E-Government Readiness in Nigeria
www.igi-global.com/chapter/web-20-ict-infrastructure-and-training-provision-for-e-government-readiness-in-nigeria/109495?camid=4v1a

New Questions for E-Government: Efficiency but not (yet?) Democracy
www.igi-global.com/article/new-questions-government/76929?camid=4v1a