Chapter LXII
Implementing a Sound Public Information Security Program

Stephen K. Aikins
University of South Florida, USA

INTRODUCTION

The evolving nature of information security threats such as cybercrime, as well as the need to ensure the confidentiality and privacy of citizen information and to protect critical infrastructure call for effective information security management in the public sector. According to Evers (2006), the FBI (Federal Bureau of Investigation) estimates that cybercrime will cost businesses an estimated $67.2 billion per year. Citizens' privacy and the security of their personal information have become issues of increasing concern as headlines of data security breaches and identity thefts abound in the mainstream media. For example, in 2005, 9.3 million U.S. citizens, about 4.25% of the population, were victims of identity theft and fraud, costing approximately $54.4 billion (Council of Better Business & Javelin Strategy & Research, 2006).

E-government applications have made it easier for citizens to conduct business online with government agencies, although their trust in the ability of governments to keep that information private is low. Considering the amount of citizen information held by governments at all levels and the steps needed to address potential homeland-security and IT-related threats to critical infrastructure, the need for effective means of safeguarding public agency data has become an issue of paramount importance. In addition, the need to ensure integrity and availability of public information resources is crucial to many government operations. As a result, several states are recognizing the importance of information security and privacy in their state IT strategic plans (National Association of State Chief Information Security Officers [NASCIO], 2006).

BACKGROUND

Almost two decades after the Computer Security Act was signed into law, federal IT security reviews indicated continuing risks to federal operations (U.S. General Accounting Office [GAO], 2000, 2001, 2002). This appears to be happening despite the escalating cost of federal IT security spending, which is expected to increase from $4.2 billion in 2003 to $6 billion in 2008 (Walker,

Copyright © 2008, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

2003). A key requirement for effective planning and management of public organizations' information security is the implementation of a public information security program.

Several public agencies such as the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), the National Security Agency (NSA), the GAO, and NASCIO have published numerous security documentations that serve as sources of reference for public organizations in managing the security of their information resources. However, a recent survey by NASCIO (2006) revealed that about 30% of the state chief information security officers (CISOs) were unfamiliar with major cybersecurity-related documents. This chapter discusses the elements of an effective information security program and how it could be implemented by state and local governments to mitigate their security vulnerabilities, threats, and exploits.

ELEMENTS OF AN INFORMATION SECURITY PROGRAM

The implementation of an effective information security program begins with a risk assessment and the development of an enterprise-wide information security plan. State and local governments should understand their environment and conduct IT risk assessment. This is done to determine their security needs and formulate plans that include strategic goals to protect critical infrastructure and citizen privacy. Once the plan is in place, an information security program that embodies security management structure and comprehensive policy, related standards, and procedural guidelines should be developed. GAO (2001) outlines the following elements of an information security program as critical.

1. Periodic risk assessment
2. Documented entity-wide security program plan
3. Security management structure with clearly assigned security responsibilities
4. Effective security-related personnel policies
5. Security program evaluation

Perform Periodic Risk Assessment

Understanding the risks of the public organization is crucial in determining the proper security policies, procedures, guidelines, and standards to put in place to ensure adequate information security controls. The IBM Foundation for the Business of Government (2002) argues a risk assessment should include a complete inventory of critical systems and assets as well as a gap analysis between the actual and ideal levels of IT security. Therefore, the risk assessment should include a review of such broad areas as employee management and training; information systems, including network and software design and information processing, storage, transmission, and disposal; and detection, prevention, and response in the case of attacks, intrusions, and failures (NSA, 2002).

Effective risk assessment should have three major components: threat assessment, vulnerability assessment, and asset identification. In a survey of State CISOs, NASCIO (2006) found that although 73% of the respondents reported they have conducted risk assessments on systems that are homeland-security-critical assets, 76 to 84% reported they have inadequate or no information regarding threats from "internal ineptitude" and "internal maliciousness," which are potentially the most dangerous aspects of security breaches. Assessing the threats posed by a malicious insider (e.g., disgruntled employee), accidental insider (e.g., poorly trained or curious employee), malicious outsider (e.g., hacker, industrial espionage), and nature (e.g., fire, flood) will be useful in identifying and assessing the government agency's vulnerabilities (Hurd 2001; NIST, 2002).

Vulnerability assessment should focus on key areas of information security, including identifi-

8 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/implementing-sound-public-information-security/21289

Related Content

Influence of IoT Policy on Quality of Life: From Government and Citizens' Perspectives
Sheshadri Chatterjee (2019). *International Journal of Electronic Government Research (pp. 19-38).*
www.irma-international.org/article/influence-of-iot-policy-on-quality-of-life/247927

Enhancing Visibility in International Supply Chains: The Data Pipeline Concept
Bram Klievink, Eveline van Stijn, David Hesketh, Huib Aldewereld, Sietse Overbeek, Frank Heijmannand Yao-Hua Tan (2012). *International Journal of Electronic Government Research (pp. 14-33).*
www.irma-international.org/article/enhancing-visibility-international-supply-chains/74812

A Paradigm Shift in Swedish Electronic Surveillance Law
Mark Klamberg (2013). *Digital Democracy and the Impact of Technology on Governance and Politics: New Globalized Practices (pp. 175-201).*
www.irma-international.org/chapter/paradigm-shift-swedish-electronic-surveillance/74574

Certificate Management Interoperability for E-Government Applications
Andreas Mitrakas (2007). *Secure E-Government Web Services (pp. 143-161).*
www.irma-international.org/chapter/certificate-management-interoperability-government-applications/28486

What Skills are Needed in an E-World: E-Government Skills and Training Programs for the Public Sector
Alexander Settles (2005). *Practicing E-Government: A Global Perspective (pp. 383-414).*
www.irma-international.org/chapter/skills-needed-world/28104