Information Security Management in Digital Government

Hui-Feng Shih
Coventry University, UK

Chang-Tsun Li
University of Warwick, UK

INTRODUCTION

Ensuring security for its information systems, including computers and networks, is a fundamental prerequisite for a digital government to function to the expectation of its people. The security problem can be "visualized" by projecting it onto a three-level hierarchy: management level, system level, and application and data level. The key elements of information security include integrity, confidentiality, availability, authentication and non-repudiation, which have to be taken into account at different levels within the hierarchy. Since there are specific articles in this encyclopedia to address the security issues at the lowest two levels, this article will focus on the management level at the top level of the hierarchy.

At the management level, the main emphases are to prevent security breaches from happening and to minimize the impact when security events happen. The decision of security investment and deployment requires clear identification of risks posed to the information systems and feasible cost analyses. In addition, to ensure that the investment and deployment are worthwhile, information security policies and procedures have to be thoughtfully devised and effectively enforced. Therefore, at the management level, *risk assessment*, *cost analysis*, *policymaking*, *procedure definition,* and *policy and procedure enforcement* have to be looked into.

RISK ASSESMENT

Risk assessment is a systematic approach to identify critical risks, analyze the impacts of the risks and mitigate them. With limited resources for putting in place a security process, a digital government has to assess potential risks to ensure that resources are deployed in an optimal manner. Therefore, the following steps, namely *risk identification*, *risk impact analysis* and *risk mitigation*, have to be taken.

- **Risk Identification:** The objective of risk identification is to delineate those risks that can have significant impact on the functionality and credibility of the digital government. Aspects to be looked into include *technical source of risks*, *procedural source of risks* and *probability of security breach* (Rajput, 2000).
    - **Technical Source of Risks:** Weaknesses and limitations inherent in the employed techniques, such as the encryption, firewall and so forth, need to be identified. For example, as computing power keeps increasing, the strength of the data encryption standard (DES) (Stallings, 1998), which has been in widespread use for some 20 years, is pushed to its limit and no longer deemed as secure for critical processes.
    - **Procedural Source of Risks:** Procedural controls in administration processes and system access processes may also have some loopholes to be covered. Personal behavior and organizational culture may also have influence on procedure and practice.
    - **Probability of Security Breach:** Probability of the occurrence of potential risks needs to be studied so that risk impact can be objectively analyzed. A model for calculating the probability of a breach occurrence can be found in Coleman (2003).
- **Risk Impact Analysis:** With the potential risks identified, impacts on the following aspects need to be analyzed.
    - **Credibility of the Government:** "Visible" security breaches, physically significant or insignificant, can harm the credibility of the government and reduce its people's confidence in it. For example, the reputation of a government's ability to protect its information or even its people may be compromised if the

Copyright © 2007, Idea Group Inc., distributing in print or electronic forms without written permission of IGI is prohibited.

images of the national flag on its governmental portals are replaced by its rival nation with the images of the latter's national flag.
- **Information Availability and Service Continuity:** 24-hours-a-day/7-days-a-week information availability and service continuity are the key requirements and characteristics that distinguish digital governments from traditional governments. Unavailability and discontinuity of information services will certainly have prominent impact on the functionality of the government, and therefore need to be analyzed.

- **Risk Mitigation:** Risk mitigation is the process of using effective controls to minimize the impact of the risks to an acceptable level. This process enables the government to determine how much risk it is prepared to take and to what extent its assets and data should be protected. To mitigate the impacts of the potential risks on the digital government, essential technological security controls need to be put in place, and procedures and practice guidelines have to be drawn up.

The level of acceptable security is determined by weighing the probability of threat against the cost of putting up resistance against the threat. Within the level of acceptable security, identifying and attempting to mitigate the risks with low probability of occurrence have insignificant value. There is a wide spectrum of implications stemming from the need for risk mitigation, such as cost, policy formulation or even cultural change among the civil servants of the digital governments.

COST ANALYSIS

Effective security mechanisms require a process that allows digital governments to determine informatively the acceptable level of security within which risks are mitigated to a minimum. Once the security level is determined, cost analysis aiming at reaching that level can then be carried out. Cost analysis includes:

- *Direct financial costs* incurred by the acquisition or lease of security assets and services, such as network monitoring devices, firewalls, encrypting routers and lease of Virtual Private Network (VPN) services. In addition to the hardware and software, a department charged with the responsibility of ensuring information security has to be established. External or independent audits also have to be involved regularly for reviewing the security practices and procedures, assessing unidentified risks, and making recommendations and reports. These all add up to a significant overhead.
- *Indirect performance costs* incurred by the incorporation of processes of authentication, administration, encryption, integrity verification, policy enforcement and so forth. Some of these processes will directly reduce the performance and efficiency of the IT systems. Some (e.g., policy enforcement, security controls and security audit) may result in rivalry between government agencies, which may cause ill effect on the performance of the government itself rather than on the information technology (IT) systems.

POLICYMAKING

Security policy is a set of rules that regulate how a digital government manages the risks and protects its data and information systems. This has to take into account the management, uses and distribution of its information and IT assets. Aspects to be looked at when formulating security policies include:

- **Standards:** Any digital government committing to information security needs to look for guidance to achieve consistent, comprehensive and assessable security. Several standards providing useful guidance are now available. BS 7799/ISO 17799 (BS 7799 Part1, 2000) is one of the most prominent standards.
- **Data Classification:** Over-protection might have negative impact on the performance of the government, while under-protection may compromise the security. Data classification facilitates selective security enforcement.
- **Regulation of Use of Data and Assets:** For example, the use of live information for development and testing should be prohibited and the use of sniffers (i.e., software or devices monitoring data flowing over networks) has to be regulated.
- **Human Rights and Privacy:** Regulations governing the protection of human rights and privacy is the part of a digital government's commitment that has to be addressed in the security policy.
- **Response to Warnings:** Digital government agencies should set up pre-defined procedures and actions to take in response to security incidents of different levels of security concerns or warnings issued by security organizations, such as the Computer Emergency Response Team (CERT), so that the agencies could respond promptly.

2 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/information-security-management-digital-government/11632

Related Content

Public Sector E-Commerce
C. G. Reddick (2007). *Encyclopedia of Digital Government (pp. 1383-1387).*
www.irma-international.org/chapter/public-sector-commerce/11685

New Directions for IT Governance in the Brazilian Government
Fabio Perez Marzulloand Jano Moreira de Souza (2011). *Applied Technology Integration in Governmental Organizations: New E-Government Research (pp. 313-334).*
www.irma-international.org/chapter/new-directions-governance-brazilian-government/49351

In-Stream Data Processing for Tactical Environments
Marco Carvalho (2008). *International Journal of Electronic Government Research (pp. 49-67).*
www.irma-international.org/article/stream-data-processing-tactical-environments/2045

The E-Governance Concerns in Information System Design for Effective E-Government Performance Improvement
Kam Hou Vat (2010). *Handbook of Research on E-Government Readiness for Information and Service Exchange: Utilizing Progressive Information Communication Technologies (pp. 48-69).*
www.irma-international.org/chapter/governance-concerns-information-system-design/36471

Smart Cities and Their Roles in City Competition: A Classification
Leonidas G. Anthopoulosand Panos Fitsilis (2014). *International Journal of Electronic Government Research (pp. 63-77).*
www.irma-international.org/article/smart-cities-and-their-roles-in-city-competition/110957