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 ASSESSMENT

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