Chapter XVI
Security and Risk Management

The value of information and knowledge is directly proportional to the risk of losing it. (Koh, 2007)

SECURITY AND RISK MANAGEMENT DEFINED

In information terms, **security** can be defined as the processes of ensuring that private information remains private and uncompromised in an atmosphere where all other information is free. Security techniques such as encryption, passwords, and firewalls are designed to prevent unauthorized access to information, to protect the integrity of computing resources, and to limit the potential damage that can be caused by attackers and intruders. The notion of a "secure computer" is relative though: the only truly secure computer is one powered down in a locked facility that no one has access to.

Risk management is the ongoing process of assessing the risk to automated information resources. It is part of a risk-based approach used to determine adequate security for a system by analysing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk (Maguire, 2002).

Exhibit 16.1.

Mini case: Loosing government data – Risking the nation

A computer hard drive containing the details of about 5000 employees of the justice system was reported missing on 7 September 2008. The justice secretary was not informed about this lost, which happened in July 2007. It was reported that the details of employees of the National Offender Management Service in England and Wales, including prison staff, were lost by private computing firm EDS. The Justice Minister was very angry at the loss and various enquiries are conducted to establish the cause of this loss.

There are various recent losses of government data in the last two years, including (1) Nov 2007: 25m people's child benefit details, held on two discs; (2)Dec 2007: 7,685 Northern Ireland drivers' details; (3) Dec 2007: 3m learner drivers' details lost in US; (4) Jan 2008: 600,000 people's details lost on Navy officer's stolen laptop: (5) June 2008: Six laptops holding 20,000 patients' details stolen from hospital; (6) July 2008: Ministry of Defence (MoD) reveals 658 laptops stolen in four years.

It is clear that the impact of the loss of government data will impose major risks to the society at all levels, raising concern on data, personal and business securities. For example, for the case on 7 September 2008, the use of a private firm in handling the data has certainly resulted in unwanted exposure. A review of the existing policy and data security procedure in handling government and sensitive data must be carried out and new, more restricted and enforced procedure must be in place in order to minimise future major risks.

Source: BBC News. Data on 5.000 iustice staff lost. 7 September 2008. UK.

PREDICTION AND IMPACT

According to the Pew Internet & American Life Project and Elon University in January 2005, two-thirds of security experts believe that the US will suffer a 'devastating' cyber attack within 10 years. The attack may hit critical infrastructure or large industries, like banking. To add another level of vulnerability into this risk, Cyota in January 2005 noted that almost half (44 percent) of online banking customers use the same password for multiple online services. Furthermore, 37 percent of online banking customers use the same password at other, less secure sites.

International Data Corporation predicted in December 2004 that revenues for antispyware software companies are expected to climb from USD12 million in 2003 to USD305 million in 2008. It is clear that with the increased adoption and utilisation of e-technology in our lives, the greater the risks it imposes on us.