In the past decade two developments have brought information security management issues to the fore. First has been the increased dependence of organizations on information and communication technologies, not only for key operational purposes but also for gaining strategic advantage. Second, abetted by information and communication technologies, the whole business model for many organizations has been transformed. Whereas in the past companies could rely on confining themselves to a particular geographical area to conduct their business, today companies are increasingly becoming location independent and are finding themselves to be strategically disadvantaged if they are confined to a particular place. The consequence of advances in information technologies and the changing boundaries of the firm have brought the importance of data and information to the fore. This is because it is information that helps companies realize their objectives and helps managers to take adequate decisions. In the business model of the past, data and information to a large extend was confined to a particular location and it was relatively easy to protect it from falling in the hands of those who should not have it (i.e. maintain confidentiality). Because information was usually processed in a central location, it was also possible to ensure, with a relative degree of certainty, that it’s content and form did not change (i.e. maintain integrity) and ensure that it was readily accessible to authorized personnel (i.e. maintain availability). In fact maintaining confidentiality, integrity and availability were the main tenants for managing security. Today because the nature of the organization and scope of information processing has evolved, managing information security is not just restricted to maintaining confidentiality, integrity and availability. Perhaps as Dhillon & Backhouse, (2000) point out, the emphasis should be on establishing responsibility, integrity of people, trustworthiness and ethicality.
Changing structures, advances in information and communication technologies and the greater reliance of companies on information indeed poses a number of challenges for maintaining good management practices. In recent years clearly organizations have fallen short of developing adequate policies to deal with the information security problems. Various authors have reported increases in incidents of computer crimes because of violation of safeguards by internal employees of organizations (as high as 80% of total computer crimes – e.g. see Dhillon, 1999a). There also seems to be a ‘policy vacuum’ to deal with information security problems. This is evidenced not only by increases in incidents of system penetration (e.g. hacking), but also in inability of authorities to establish adequate basis to deal with such computer crimes. One example is the case of Randal Shwartz where there were difficulties to establish whether illicit use of computers by Shawartz amounted to an occurrence of a computer crime (Dhillon and Phukan, 2000).

Advances in information technologies have introduced a yet another kind of a problem for organizations which many classify as ‘input crimes’ (Dhillon, 1999b). In one case a former employee of a wholesaler was convicted under the UK Computer Misuse Act when he obtained for himself a 70% discount when the regular staff of the wholesaler were otherwise engaged. Given the increased dependence of businesses on computers, one would assume that most companies would have well established contingency and disaster recovery plans. Unfortunately research seems to suggest otherwise. Based on survey findings Adam & Haslam (2001) suggest that adequate importance is not being placed on disaster recovery planning. Many managers tend to think that disaster recovery planning is an insignificant issue and hence prefer to concentrate on projects that generate revenues.

**THE CHALLENGES**

It goes without saying that, incidents of computer crime, information security problems and information technology enabled frauds have been on the increase. And any attempt to deal with the problem demands an adequate understanding of the challenges that exist in the new millennium. Such challenges can be classified into four categories:

- The challenge of establishing good management practices in a geographically dispersed environment and yet being able to control organizational operations.
- The challenge of establishing security policies and procedures that adequately reflect the organizational context and new business processes.
- The challenge of establishing correct structures of responsibility, given the complex structuring of organizations and information processing activities.
- The challenge of establishing appropriate information technology disaster recovery plans.

Numerous studies (for a summary and review see Mikko Siponen’s chapter in this book, besides Dhillon et al, 1996; Dhillon, 1997) have indicated that there is a problem in managing information security especially with respect to regulating the
Related Content

Memory-Based Antiforensic Tools and Techniques
[www.igi-global.com/article/memory-based-antiforensic-tools-techniques/2478?camid=4v1a](www.igi-global.com/article/memory-based-antiforensic-tools-techniques/2478?camid=4v1a)

Secure Data Hiding Using Eight Queens Solutions
[www.igi-global.com/article/secure-data-hiding-using-eight/75322?camid=4v1a](www.igi-global.com/article/secure-data-hiding-using-eight/75322?camid=4v1a)

Global Information Security Factors
[www.igi-global.com/chapter/global-information-security-factors/62721?camid=4v1a](www.igi-global.com/chapter/global-information-security-factors/62721?camid=4v1a)

Building an Ethical Framework for Decision Making
[www.igi-global.com/chapter/building-ethical-framework-decision-making/28497?camid=4v1a](www.igi-global.com/chapter/building-ethical-framework-decision-making/28497?camid=4v1a)