Poster paper

An Overview of Alternative Approaches for Managing Information Security

Mehdi Asgarkhani
Christchurch Polytechnic Institute of Technology
Christchurch, NZ
AsgarkhaniM@CPIT.ac.nz

Recent advancements in Information and Communications Technology (ICT) have resulted in the staggering growth of global computer networks – which in turn has made it possible for critical information to be disseminated across these global networks. This phenomenon has resulted in a paradoxical environment. More specifically, innovative enterprises are now given the opportunity in which to use globally connected networks and the Internet so as to initiate (on an ongoing basis) new and exciting approaches to conducting business. Yet, there is a danger. The networking structures are now complex and diverse. Organisations are exposed to greater risks - in particular that of increasing demand on the bandwidth and the security of business information.

Within the past few years, we witnessed numerous Denial of Service (DoS) attacks on well-known sites (such as Amazon, Yahoo, E*Trade and the CNN to mention a few) alongside intensified widespread virus attacks throughout 2003 and 2004. The increasing rate of reported cyber crimes and information security problems suggest that highly structured and technical traditional methods for managing information security are no longer effective. Today, information is viewed as the most valued asset within organizations. Protecting corporate information is a business requirement and the process of security is a business process.

A preliminary review of literature (reports, cases and so on) indicates that a wide range of tools, techniques, policies and strategies have been considered in order to combat the security risks. However, numerous cases appear to be confined to one aspect of information security management. More specifically, security is viewed as technical infrastructure and hardware/software security solutions (such as: virus scanners; encryption techniques; intrusion detectors; and firewalls to name a few) for computer networks. There is little or no mention of other underlying issues (such as: culture; attitudes; management support; strategic approach and so on) that may need to be considered in managing information security.

The focus on technology is not sufficient to produce results. The benefits of advanced technological tools can only materialize when they are introduced as part of a well-planned and properly supported environment. Successful security solutions need to be reliant on the development of a strategy that optimises the application of technology through giving consideration to other issues such as: culture change; employee education; sound security policies, well prepared security plans and risk management (including transfer of risk via security insurance).