

## Why is Information Security Important?

If there is a weakness in your IT security system, wouldn't you prefer to find it before someone else does?

Imagine waking up to discover that your IT systems have been hacked. Your company's financial results have been leaked to the media; your confidential business plans have been compromised; your employees' personal files have been posted on the internet. The market loses confidence in your organisation, your share price takes a dive, and your directors are found to be personally responsible for inadequate risk management practices.

Sound scary? It is. An extreme example? Perhaps. But even a small scale security breach could leave your business without access to its critical IT systems for hours or days.

Every organisation uses information, most are dependant on it. Information is an asset that, like other important business assets, is essential to your business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment, where information is now exposed to a growing number and a wider variety of threats and vulnerabilities. Causes of damage such as malicious code, computer hacking, and denial of service attacks have become more common, more ambitious, and increasingly sophisticated.

Information security is not an 'IT problem', it is a business issue. Obviously compliance with legal and regulatory requirements is important. It provides a very good reason for reviewing your information security practices, but it should not in itself be the sole or even the main driver. If a business wishes to survive, let alone prosper, it must grasp the importance of information security and put in place appropriate measures and processes.