

## Managing information security

Dependence on information systems has grown in all areas of life, and to a great extent this has meant increasing dependence on computerised information systems. Recent trends of working,

**Information security** is the preservation of confidentiality, integrity and availability of information.

- Confidentiality - ensuring that information is accessible only to those authorised to have access.
- Integrity –safeguarding the accuracy and completeness of information and processing methods.
- Availability -ensuring that authorised users have access to information and associated assets when required.

such as the greater availability and use of palmtop or laptop computers, bring with them new risks not faced previously, such as being able to lose or have stolen prodigious quantities of data, some of which may be confidential or sensitive. The growth of the internet and increased inter-networking within organisations (as well as wireless networking) has meant that our information systems are now much more vulnerable to attack, potentially from anywhere in the world. This includes the threat of “hacking” (i.e. unauthorised access to computer systems), damage by computer viruses, and computer-assisted fraud. In addition, damage can be caused to computerised information systems as a result of malfunction, and accidental damage such as flood or fire.

### Where do you start?

The process of managing information security should start by each organisation assessing its own security requirements. This should involve an assessment of organisational risks generally and specifically in relation to information processes developed by the organisation to meet its own operational requirements, as well as consideration of legal, statutory, regulatory and contractual requirements.

### BS ISO/IEC 17799 – Information Security Management

The British Standards Institution has issued, as BS ISO/IEC 17799:2005, a revised Code of Practice for Information Security Management. This consists of three parts – Part I consists of the Code of Practice itself, Part II consists of a Specification for information security management systems and Part III contains guidelines for information security risk management. The Code of Practice was originally issued in 1995, and the current revision was issued in 2005.

Part I gives recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organisation. It is intended to provide a common basis for developing organisational security standards and effective security management practice and to provide confidence in inter-organisational dealings. Although the Code of Practice makes no specific reference to charities or non-profit organisations, it provides an accredited framework through

In the context of information security, the following definitions may be helpful:

#### Risk assessment

Assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence.

#### Risk management

Process of identifying, controlling and minimising or eliminating security risks that may affect information systems, for an acceptable cost.

which they could demonstrate to beneficiaries, donors and funders that the organisation has met its governance responsibilities in respect of information security.

## Controls

Although each organisation's security needs are different, the Code of Practice identifies ten controls that can be considered as a good starting point for any organisation for implementing an information security strategy. Seven of these controls can be categorised as 'best practice' measures:

- An information security policy document.
- Allocation of information security responsibilities.
- Information security awareness, education and training.
- Correct processing in applications.
- Technical vulnerability management.
- Business continuity management (e.g. procedures to assist in the recovery of essential systems from an unforeseen disaster).
- Management of information security incidents and improvements.

The remaining three 'starting point' controls can be categorised as 'legislative':

- Compliance with intellectual property rights (e.g. control of software copying).
- Safeguarding of organisational assets (including issuing guidelines on the retention, storage, handling and disposal of records and information).
- Compliance with data protection and privacy of personal information requirements (e.g. Data Protection Act 1998).

The Code of Practice emphasises that, although the 'starting point' controls apply to most organisations and in most environment, they should not be considered a substitute for controls based on an organisational risk assessment.

## Critical success factors

The Code of Practice also identifies ten 'critical success factors' which experience has shown to be associated with successful implementation of information security within an organisation:

- Security policy, objectives and activities that reflect business objectives.
- An approach to implementing, maintaining, monitoring and improving information security that is consistent with organisational culture.
- Visible support and commitment from all levels of management.
- A good understanding of the organisation's security requirements, risk assessment and risk management.
- Effective marketing of security to all managers, employees and other parties.
- Distribution of guidance on information security policy and standards to all managers, employees and other parties.
- Provision to fund information security management activities.
- Providing appropriate awareness, training and education.
- Establishing an effective information security incident management process.
- A comprehensive and balanced system of measurement which is used to evaluate performance in information security management and feedback suggestions for improvement.

In addition to the 'starting point controls', the Code of Practice identifies over a hundred possible controls, which should be considered in relation to the organisation's own ways of working, type of business and its own risk assessments. These fall into ten sections in the Code of Practice,

covering, for example, asset management, human resources security (e.g. threats to and from personnel), physical and environmental security and operational measures such as incident procedures and segregation of duties. The Code of Practice devotes a great deal of attention to IT systems, including access control policy, electronic communications and systems maintenance.

## Conclusion

The Code of Practice can either be used as a framework within which to develop an informal standard of Information Security Management, or as a way of developing Information Security Management Systems (ISMS) for which certification of compliance with BS ISO/IEC 17799 can be sought. At the time of writing, only around 250 organisations in the UK have received certification (see <http://www.xisec.com/>). It remains to be seen whether compliance will become a widely used benchmark for charities or non-profit organisations, but the principles contained within the Code of Practice are ones which arguably fall within the governance requirements of any charity.

## Useful publications and links

From The Stationery Office [www.tsoshop.co.uk](http://www.tsoshop.co.uk)

- BS ISO/IEC 17799:2005 Information Technology. Code of Practice for Information Security Management (ISBN 0580462625) £110.00
- BS ISO/IEC 27001:2005 Information Technology - Security Techniques - Information Security Management Systems – Requirements (ISBN 0580467813) £90.00
- BS 7799-3:2006 Risk Management (Applied to Information Security) ISBN 0580472477 £70.00
- BIP 0071:2005 Information security management systems (ISMS) certification. Guidelines on requirements and preparation for certification based on ISO/IEC 27001:2005 (BS 7799-2:2005) ISBN 0580460029 £25.00

DTI Information Security page <http://www.dti.gov.uk/sectors/infosec/index.html>

The Information Commissioner's Office <http://www.ico.gov.uk>