

FINANCIAL DIRECTOR BRIEFING information security

TODAY'S CHOICE IS TOMORROW'S MUST

The British Standard code of practice for information security in business, BS 7799, was originally published in 1993 and revised in 1999. But only the largest companies have adopted it to date.

Compliance with BS 7799 is increasing as regulations such as the Data Protection Act, Basel II and Sarbanes-Oxley push data security up the boardroom agenda.

Much of the following advice is taken from an ICAEW publication, *A Management Guide to BS 7799*, which sets out the framework for compliance. The code of practice highlights eight measures that are considered essential requirements or fundamental building blocks for information security. The ICAEW says companies should consider these measures first before implementing BS 7799.

Measures to consider

1. When creating an information security policy document, it should include a definition of information security, a statement of management intention, and an explanation of specific security procedures, standards and requirements. The policy should be subject to review.
2. Allocation of information security responsibilities can be covered by the policy and supplemented with details for specific sites, services or applications. Manager responsibility should be stated clearly.
3. Information security education and training should apply to all employees and third-party users.
4. There should be a formal procedure for reporting security breaches, which should apply to all staff and contractors. These will

report any potential breach of security to a single focal point.

5. There should be a business continuity planning process to assist in the recovery of essential systems from an unforeseen disaster. This should include production of a plan and the testing and updating of the plan.
6. There should be a policy to preserve intellectual property rights including copyright. This requires control of software copying.
7. Organisational records should be safeguarded. Important records from an organisation must be protected from loss, destruction or falsification. Guidelines should be issued on the retention, storage, handling and disposal of data.
8. Compliance with the Data Protection Act 1998, or its equivalent in other countries, is a must. Individual privacy rights must be respected.

Once these measures have been considered, BS 7799 sets out 10 areas of control that must be addressed to ensure compliance.

Areas of control

1. Create an information security policy that sets a clear management direction and demonstrates support for information security through the publication of the policy across the organisation.
2. Organisational and managerial aspects of security include, for a large organisation, setting up information security forums to ensure high management involvement and to co-ordinate security across the organisation. If any third parties have access to the organisation's information, the risks should be assessed and controlled while the contracts with

the third parties should specify the security conditions which apply.

3. Inventories of information, software, physical assets and services should be created. Information should be classified according to its need for confidentiality, integrity and availability. There is no standard for classification, although the DTI has suggested three levels in its booklet, *Protecting Business Information (Keeping it Confidential)*.
4. Personnel security covers threats to, and from, personnel. The code recommends recruitment screening, a confidentiality agreement for each member of staff, and job descriptions which include security obligations. Security incidents must be reported and a disciplinary process should be invoked for staff members who violate policy and procedures.
5. Keep the premises, people and the assets within them safe. Its objectives include preventing unauthorised access, damage and interference, with special emphasis on IT facilities.
6. Management of operations and communications include the operating procedures that should be in force, the reporting of incidents, segregation of duties and how to deal with incidents. The planning, acceptance and change of systems is also covered. The section describes the actions to be taken against malicious software (for example, viruses) back-up, logging and general housekeeping.
7. System access control include recommendations for a documented access control policy and user access management. The latter covers registration of users, password management, and the allocation and review of user access rights. Individual user responsibilities include care over password use and the logging off of unattended equipment.

8. System development and maintenance include IT systems requirement, encryption and technical reviews.
9. Disaster recovery or contingency planning requires plans to be drawn up, tested and updated.
10. Compliance means compliance with security policy, the law and the needs of audit. The legal requirements include safeguarding of organisational records (the Companies Act 1985), data protection, and the Computer Misuse and Copyright, Designs and Patents Acts (1990 and 1988).

Comment

Michael Clinch, partner at Hextalls law firm, says the current focus on corporate governance, regulation and information security means that standards such as BS 7799 are likely to become mandatory. "The recent trend for information technology and compliance systems in specific sectors, such as Basel II, have refocused industry attention on the importance of information security and management," says Clinch.

"In time, companies are likely to find that adherence to accepted name standards will, in effect, be imposed as a result of pressure from buyers. The difficult task will be in attempting to reconcile the various regimes and for suppliers to juggle their various certifications."

Tom Berry

A wide range of Briefings can be found at www.financialdirector.co.uk/briefing

Useful links

- Information about BS 7799 is at www.bsi-global.com
- A *Management Guide to BS 7799* can be found at www.icaew.co.uk
- Contact Michael Clinch at msc@hextalls.com