



BS 7799 has been gaining momentum in both the public and private sectors. Government mandates and the Turnbull Report are making certification more attractive to organisations keen to improve information security. Maria Dennis, training manager of Red Island Consulting, unravels some of the common misconceptions surrounding the standard and explains how, with the right guidance, it can bring significant benefits

Towards the end of the 1980s information security was a hot topic. The DTI was asked to provide guidance on security evaluation criteria to vendors of IT security products. At the same time, there was a demand from users for a code of practice on information security. In response to this, DTI created the 'Users Code of Practice', first published in 1989. As with the evolution of most standards, this code of practice underwent several reviews and amendments until it finally morphed into what we know today as BS 7799. But what is it exactly?

insecure, me?

Red Island Consulting are BS 7799 specialists. Experienced in both private and public sector, they are members of the BSI Associate scheme, official auditors for NHS-net connectivity and official suppliers to government being S-Cat listed as part of the VantagePoint Consortium. They are also suppliers of information security training services. For further information go to www.redisland.co.uk or t: 020 7422 7159.



What is BS 7799?

Essentially, BS 7799 provides a specification for the design, development and implementation of an information security management system, just as ISO 9001 does for a QMS. It works on the premise that information is a significant asset to any organisation which therefore needs to be clearly identified and managed. Ascertaining risk levels lies at the centre of the standard. The onus is on the organisation to accurately identify its information assets and all possible threats to the security of that information.

Correctly identifying the information assets is one of the more challenging requirements of the standard. This is why many organisations use a consultant, as it is worthwhile to get an objective external view at this stage. It is then at the discretion of the organisation as to how they choose to manage the risk. They may decide to accept it, to mitigate it, to transfer it to a third party or to implement appropriate controls depending on the type of threat.

The main reason for having an information security management system is to ensure the confidentiality, availability and integrity of information. As we use and rely on computers more and more, there is a common misconception that the information system is the information. Information is held, stored and transmitted in many other media and these are all subject to the need for management and control: eg an air traffic control system is vital, but the critical information is relayed from ground to air by the operator talking to the pilot. This is also something that needs to be taken into account when identifying the information assets.

Implementation

For ease of understanding, BS 7799 can be grouped into the following key activities:

- secure management commitment
- identification of information assets, assess and manage the risk
- develop policies and procedures to effect controls

- assign roles and responsibilities
- inform and educate the user base
- monitor and maintain the system

There are definite parallels between BS 7799 and ISO 9001. In fact, the 2002 revision of BS 7799 was undertaken to bring it into line with the other management system standards. The latest revision even includes the plan-do-check-act model. Those organisations already certificated to ISO 9001 will probably already be committed to the process approach and be familiar with a management system's terminology.

How safe is your staff?

The key challenges in implementing BS 7799 lie in correctly identifying the information assets, assessing the risk's business impact, and developing a culture of awareness around information security. This last point is extremely significant. The unconscious incompetence of the user base is frequently cited as a major threat. While it is easy to relate to the threat posed by viruses and hackers, it is much more difficult to see the threat posed by your own staff.

As an example a hospital employee was talking with absolute candour about how he had accessed his girlfriend's medical records. He had no idea that this was a breach of confidentiality. There are countless incidences of staff downloading screensavers from the internet unaware that doing so could import a virus and corrupt the whole network. Another organisation's reputation suffered from the contents of a highly sensitive fax containing competitor information, that arrived on the wrong desk; the sender was unaware of the 'safe haven' procedure which requires them to ensure that the fax goes to a machine designated to receive sensitive material. Another example is a case of someone applying for a new job with a competitor and taking the entire customer database

This is just the tip of the iceberg. Without policies and procedures in place it is the CEO who is responsible; an individual is not liable if it is not company policy.

Why do it?

Depending on the industry, organisations usually embrace the standard either because they feel they have to or because it is good for business. In the commercial sector there are several drivers. For listed companies there is the influence of corporate governance and the Turnbull Report. And although companies are not legally required to comply with the Turnbull Report, there is a fiduciary duty. The implication being that directors could find themselves personally liable.

In relation to the security of information assets, the Turnbull Report states that 'a company's internal control system encompasses the policies, processes, tasks, behaviours and other aspects of a company that, taken together:

- facilitate its effective and efficient operation by enabling it to respond appropriately to significant business, operation, financial, compliance and other risks to achieving the company's objectives. This includes the safeguarding of assets from inappropriate use and from loss and fraud, and ensuring that liabilities are identified and managed
- help ensure the quality of internal and external reporting. This requires the maintenance of proper records and processes that generate a flow of timely, relevant and reliable information from within and outside the organisation
- help ensure compliance with applicable laws and regulations'

A key element of the Turnbull Report is the onus on directors to manage risk. Are risks adequately identified and assessed on an ongoing basis? Are there clear strategies for dealing with risk and are there specific arrangements for monitoring and reporting to the board?

Turnbull and friends...

The UK government has embraced Turnbull and all public sector and non-departmental public bodies have had to adopt the principles of the report. In addition to Turnbull, there is a raft of legislation that



relates to the management of information, such as the Data Protection Act, the Computer Misuse Act, the Freedom of Information Act and the Human Rights Act.


One of the significant benefits of BS 7799 is that it incorporates Turnbull's requirements as well as requiring organisations to comply with other relevant legislation. The UK government has recognised its value as a code of practice and has mandated that all central and local government must demonstrate compliance by March 2004. Additionally, the NHS Information Authority has advised that all NHS organisations should aim for compliance by March 2004. Consequently BS 7799 has become a must-have for public sector contracts.

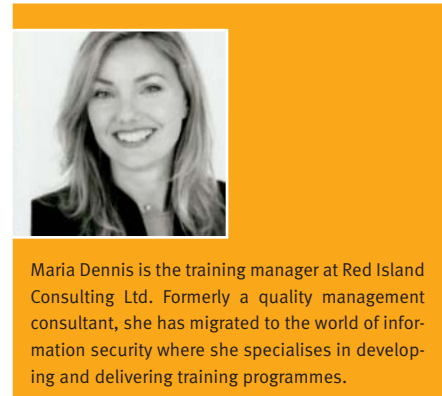
With government and the public sector firmly embracing BS 7799 and listed companies increasingly adopting it, the impact on the supply chain is inevitable.

Register the benefits

Apart from the obvious security benefits, one of the most significant consequences of implementing BS 7799 is that an organisation has, usually for the first time, a register of all its information assets. This is something that has been overlooked for a long time. The risks incurred from loss of confidentiality, integrity or availability of information are considerable. By taking information security on board, there are potentially huge savings in terms of protecting against financial loss, loss of reputation, loss of customers and damage to your brand. In addition, BS 7799 communicates a powerful message to the market: you are an organisation that takes its corporate responsibilities seriously.

While BS 7799 does not negate legal obligations, it does provide a framework for systematically managing information security risks. It is a means of developing

and embedding a security culture. And remember: your people may be your biggest asset but they can also be your biggest threat 



Maria Dennis is the training manager at Red Island Consulting Ltd. Formerly a quality management consultant, she has migrated to the world of information security where she specialises in developing and delivering training programmes.

BS 7799 the facts

BS 7799 (Part 1), the code of practice for information security management, was first published in February 1995. It was significantly revised and improved in May 1999 and later published by ISO/IEC in December 2000 to become the international code of practice ISO/IEC 17799:2000.

BS 7799-2:2002 (Part 2) is a standard specification for an information security management system (ISMS). Senior management use ISMSs to monitor and control their security, reducing long-term business risks by preventing and minimising the impact of security incidents. ISMSs also ensure that security continues to fulfil corporate, customer and legal requirements.

Both ISO/IEC 17799:2000 and BS 7799-2:2002 provide an all-inclusive coverage of information security issues. The latter defines the security management processes for an ISMS and the former defines management controls to support the implementation of these processes.

Japan	225	Taiwan	7
UK	118	Hungary	6
Korea	20	China	5
Germany	17	USA	5
India	16	Sweden	4
Hong Kong	15	Austria	3
Italy	12	Iceland	3
Singapore	10	Brazil	2
Finland	8	Denmark	2
Norway	8	Greece	2
Australia	7	Mexico	2
Ireland	7	Switzerland	2

© ISMS International User Group 2002-2004

Currently the certification is undergoing transition from BS7799-2:1999 to BS7799-2:2002. Certificates have only been awarded against BS7799-2:2002 since

5 March 2003, and all BS7799-2:1999 certificated ISMSs must be recertificated to BS7799-2:2002 by 5 March 2004.

Registration around the globe

This register has been produced in cooperation with an international network of certification bodies, the DTI and the ISMS International User Group (IUG) (the profile for Japan includes JIPDEC ISMS certificates). The total number of BS 7799 certifications worldwide is 513 (as of January 2004). The table below shows where the greatest number of certifications are.

Further details of ISMS/BS 7799 can be found on the official register website www.xisec.com This table is © ISMS International User Group 2002-2004