LEADING FIRMS' EXPERIENCE IS A CATALYST FOR NEW INFORMATION SECURITY CODE

Any organization seeking to develop a written data security policy would benefit from The Code of Practice for Information Security Management published on September 30th by the UK's Department of Trade and Industry. This code implements the requirements of existing national data protection laws. Also it allows companies to plan ahead to fulfill the requirements of the forthcoming European Union's directive (Article 17).

Need for an information security policy

Information security must ensure:

- **confidentiality:** to protect personal and other sensitive information from unauthorised disclosure;
- **integrity:** to safeguard accuracy and completeness of information and computer software; and
- **availability:** to ensure that information and services are available to users when required.

Because the threats to IT systems are likely to become more widespread and increasingly sophisticated, there is an urgent need to maintain data confidentiality, integrity and availability.

This Code of Practice is the result of six months of activity by the Department of Trade and Industry (DTI), the British Standards Institution and eight major UK and international companies: The BOC Group, British Telecommunications, Marks and Spencer, Midland Bank, Nationwide Building Society, Shell International Petroleum, Shell UK and Unilever. The Code is based on a compilation of the best information security practices developed and applied by these companies. The Code provides users of personal data with a good starting point on which to build information security practices.

The aims of the Code of Practice

1. To provide a common basis for companies to develop, implement and measure effective security management practice.
2. To provide confidence in inter-company trading.
3. To be used as a reference document to identify the measures required for particular issues or specific areas of responsibility.

The persons targeted by the Code of Practice are managers and employees responsible for initiating, implementing and maintaining information security within their organisations.

Part I is an introduction to the Code and explains its background, status and how it should be used. Although the Code of Practice is intended to be as comprehensive as possible, and to serve as a single reference point for identifying the range of information security controls required, it acknowledges that not all of the controls described will be relevant to every situation. Every user of the Code of Practice will have to adapt it to take into account its local environment and technological limitations.

Part II of the Code is ten chapters long, and establishes around 100 individual security controls under 10 major headings. These were based on the security categories commonly used by the companies involved in drawing up the Code.

1. Security policy
2. Security organisation
3. Assets classification and control
4. Personnel security
5. Physical and environmental security
6. Computer and network management
7. System access control
8. System development and maintenance
9. Business contingency planning
10. Compliance.

Under each category a comprehensive set of security controls is given which are subsequently divided into a number of logical groups. A concise summary of the overall objective and scope of the logical controls is given at the beginning of each group's section.

As not all the controls are applicable to every IT environment, the Code of Practice sets out ten especially important key controls. These are considered to be mandatory, such as legislative requirements, or fundamental building blocks for information security, for example security education.

Starting point for information security management

These key controls are a good starting point for information security management:

1. Information security policy documents
2. Allocation of security responsibilities
3. Information security education and training
4. Reporting of security incidents
5. Virus controls
6. Business continuity planning process
7. Control of copying of proprietary software
8. Safeguarding company records
9. Compliance with data protection legislation
10. Prevention of misuse of IT facilities
11. Compliance with security policy.

As part of the introductory section of the Code of Practice, advice is given on how to establish an organisation's security requirements, how to assess security risks, and how to develop the organisation's particular corporate guidelines.

Chapter I: Drawing up a written policy

The starting point of an information security policy is to demonstrate the need for management to set a clear direction and pledge its support by issuing a company information security policy. The first step is to draw up a written policy statement, which is available to all employees responsible for information security. The Code of Practice determines the minimum requirements of such a document.

Chapters 2 to 4: Assigning responsibilities

Management will need to assign responsibilities for protecting major information assets both within the company and when dealing with business partners and third parties.

Chapter 5: Physical and environmental security

This chapter outlines how management should deal with sensitive data and business-critical computer systems in order to provide physical protection from unauthorised access, damage and theft.

Chapter 6: Operational practices

This is for computer and network management. It deals with the wide range of practices that should be undertaken to provide good housekeeping controls, operational procedures and responsibilities for the security of computers and networks.

Chapter 7: System access control

The objective is to devise a proper policy to prevent unauthorised access to computer services and data. This chapter describes the need to establish clear policies for accessing and sharing computer systems and databases and to set up the technical controls to prevent unauthorised access. It tells management how to do this at a number of levels ranging from procedures for administering access rights of users, to more sophisticated measures needed to control access in the most complex networking environment. It deals, among other things,with:

1. Document access control policy
2. User access management
3. User registration
4. Privilege management
5. User password management
6. User responsibilities
7. Safeguard of unattended user equipment
8. Network access control
9. User authentication

10. Terminal identification.

Chapter 8: Security controls in new systems

This chapter aims to demonstrate that security is most effective and least expensive when built prior to the development of IT systems. It tells management how to build security controls into new computer systems and how to protect the systems development process itself.

Chapter 9: Business continuity plans

This chapter's main purpose is to prepare the company for interruptions to business activities. The continuity plan process is required to protect critical business processes from major failures or disasters.

Chapter 10: Compliance requirements

Management needs to consider compliance, including a wide range of statutory and contractual requirements. In the UK, the laws that apply to computers include the Companies Act 1985, the Copyright, Designs and Patent Act 1988, and the Data Protection Act 1984. The chapter is very concise and acknowledges that advice on specific legal requirements should be sought from the company's legal advisers.

Code to become an International Standard?

It is intended that the Code will become a British Standard. In due course, it might form the basis of an International Standard.

Code helps compliance with data protection law

In relation to compliance with the UK Data Protection Act's eighth data principle (personal data must be kept secure from unauthorised access, alteration, loss or disclosure), the Code could constitute a benchmark for Data Protection Officers in their endeavours to comply with the Data Protection Act.

The Code is straightforward, not excessively technical, providing a well-balanced understanding of the practical measures that need to be taken to ensure an adequate level of security. As the Code defines fundamental requirements or key controls that are considered mandatory, it provides a good starting point for both small and large companies needing to implement information security measures.

Copies of the Code and complementary management guides can be purchased from BSI Publications, Customer Services, Linford Wood, Milton Keynes, MK14 6LE, UK. Telephone 0908 221166. A publicity flyer with details is available from the DTI. Telephone: 071 215 1316.

This report was written by Dr. Deborah Fisch Nigri, a Privacy Laws & Business researcher.