What's the 'missing link' of information security?

This guide offers an overview of what the Data Protection Act (DPA) requires in terms of security. It aims to help Corporate Security Directors and other heads of security decide how best to manage the security of the personal (and other) data their businesses hold by emphasising the importance of putting into place management/organisational security measures, as well as physical and technical/cyber security measures.

The DPA says that *"appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."*

In practice this means businesses must have appropriate security in place to prevent data being accidentally or deliberately compromised. In particular, it means that every business needs to:

- design and organise its security to fit the nature of the data held and the harm that may result from a security breach
- be clear about who is responsible for ensuring information security
- make sure it has the right physical, technical/cyber security and management/organisational security measures; and
- be ready to respond to any breach of security swiftly and effectively

Why worry about information security?

Information security breaches can (and often do) cause real harm both to a business and to people whose data has been compromised.

Recently, several high-profile losses of large amounts of personal data have brought attention to the issue of information security. These incidents, which are becoming very common, have made it clear that information security is much more than simply a matter of physical and technical/cyber compliance and that if personal data is not properly safeguarded, this can seriously damage a business.

What kind of security measures are appropriate?

In general terms, which security measures are appropriate will depend on circumstances, but there are several areas every business should focus on. Of course physical and technical/cyber security measures are essential, but management/organisational security measures are equally important in protecting data.

Unfortunately, such measures, which focus on having robust policies, reliable, well-trained staff (who think and care about information security) and third security,
are sometimes not given enough consideration or even overlooked altogether.

Policies

Every business should have a comprehensive suite of policies that provide high-level statements of commitment on how it will achieve outcomes, as well as strategies for dealing with operational issues.

Policies may be public facing statements of a businesses' commitment and approach to the collection and use of data or an internal policy directed at telling staff how personal data collected should be handled. Policies should be used to foster certain behaviours, limit negative actions or drive forward particular good. A policy can, therefore, be a guide to action with detailed information on the steps to achieve the objective of the policy being delivered by separate procedures.

Staff

It is vital that staff understand the importance of protecting personal data; that they are familiar with the security policy of the business and that they put its security procedures into practice. This means that every business should provide appropriate initial and refresher training and this should cover:

- the business's duties under the DPA and restrictions on the use of personal data
- the responsibilities of individual staff members for protecting personal data, (including the possibility that they may commit criminal offences if they deliberately try to access, or to disclose, information without authority)
- the proper procedures to use to identify callers
- the dangers of people trying to obtain personal data by deception (for example, by pretending to be the person whom the information is about or by making "phishing" attacks) and
- any restrictions a business places on the personal use of its computers by staff (to avoid, for example, virus infection or spam).

Third party security

Businesses may use third parties to do something with personal data on their behalf. (These third parties are known as 'data processors'). This often causes security problems and particular care is needed because the business (and not the data processor) will be held responsible under the DPA for what the data processor does with the personal data.

The DPA contains special provisions that apply in these circumstances. It says that, where a business uses a data processor:

- it **must** choose a data processor that provides sufficient guarantees about its security measures
- it **must** take reasonable steps to check that those security measures are being put into practice; and
- there **must** be a written contract setting out what the data processor is allowed to do with the personal data and that contract must also require the data processor to take the same security measures as the business would have to take if it were processing the data itself.

Examples of data processors are outsourced payroll and IT support providers.

Governance and accountability

The value of taking such security measures in underwriting legal compliance can be seen looking at the Information Commissioner's Office, ('ICO's) approach to auditing compliance and enforcing the law.
In assessing the level of compliance by an organisation, the ICO will focus, amongst other things, on the role of governance and accountability and the level of any formal action it takes will be strongly influenced by the presence or absence of polices. The ICO has pointed out on many occasions how a breach could have been avoided if the organisation concerned had put adequate policies in place.

Governance and accountability will become even more important when the General data protection Regulation ('GDPR') comes into effect on 25 May 2018. The GDPR includes provisions that promote accountability and governance. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's requirements elevate their significance.

All businesses will have to put into place (and be able to demonstrate that it has done so), adequate governance and accountability arrangements. In practice this will mean that management/organisational security measures will be an essential and crucial part of any businesses' information security measures, alongside physical and technical/cyber security measures.

Where can I get further help and advice?

Please click here mail@securityinfoportal.co.uk

Security Info Portal bought to you by

Harper Morgan
Oast House
Stapeley Manor Farm
Long Lane
Odiham
Hampshire
RG29 1JE

Main Line: +44 (0) 1256 862599
Sales Line: +44 (0) 1256 862074
www.HarperMorgan.com
www.SecurityInfoPortal.co.uk