CHAPTER 2: IT'S NOT IT

The key message in this chapter is that an effective Information Security Management System (ISMS) needs to address issues relating to personnel, facilities, suppliers and cultural issues, in addition to the obvious area of information technology, and so information security is a topic that goes well beyond the remit of IT, whether that be the equipment, department or service[1].

Having identified what information security is, and recognising it as something worth being concerned about, the next stage is to determine exactly what areas and aspects of the organisation will be affected.

Starting with the source of the challenge, we need to consider the 'external and internal issues' that are likely to affect our business, 'interested parties' (e.g. regulators and clients) and information security requirements of these parties to ensure that the ISMS is relevant to our organisation and provides an assurance that is appropriate to our stakeholders. It is then a case of including everything that can affect our information, which means including all the equipment on which that information is held, how

[1] Cyber security, a discipline closely related to information security, is defined as encompassing the protection of all electronically facilitated business information and processes, and all information and control systems. As such, it encompasses the fields of information assurance and information security across technical, people and physical domains (PAS 555:2012).

it is moved/transmitted and any aspects of the business that can affect the information, equipment and related processes. This means we need to set both physical and logical perimeters for our ISMS.

In practice this means that it is necessary to consider the dependencies and interfaces of all aspects of the management system and the information it controls. For example, if we consider information that is sent by courier to another office of the same organisation then we need to include the selection of the courier company and the security requirements placed on the courier through the contract.

With regard to confidentiality it is necessary to consider everyone who has access to the information and the equipment on which it is stored. This is likely to include cleaners and maintenance staff, in addition to directly employed staff.

The system also needs to address the management of information in different formats, including electronic form and hardcopy documents. With information in transit — whether it be in the form of papers being taken home for reviewing the night prior to a meeting, or records being sent to archive — it becomes obvious that hardcopy documents warrant a similar degree of protection to electronic copies. If a trade secret is accessed by a competitor it does not matter whether it is in an e-mail attachment or printed on a piece of paper: the information that was meant to be kept confidential is in the hands of, or available via a means that results in unauthorised access and so any value attached to maintaining its

confidentiality is compromised. The value of information is in its content, not in the format it is stored or available in.

Considering these issues, one way or another the ISMS needs to define how it addresses relationships with suppliers, business partners, customers and staff. Of course, the facilities and equipment used to protect and provide information are of equal importance, and also need to be considered within the scope of the ISMS.

In defining the remit of the ISMS this way the organisation is stating the scope of the assurance the system provides. Given the personnel, facilities, suppliers and cultural issues that need to be considered and addressed within the system, it is obviously a topic that goes well beyond the remit of the IT department.