CHAPTER 1: INFORMATION SECURITY – WHAT'S THAT?

To develop an understanding of what information security means, let's consider something that we all understand the value of: money.

Considering the various aspects of how you look after and use your money, the following emerge as valuable and worthy of note:

Aspect One

You do not want other people spending your money, or at least anyone not given your permission to spend it. This means limiting access to your money, or, when considering information instead of money, keeping it confidential.

This makes good sense, and at first pass may seem to be the only thing that matters. However, if restricting access to your money is all that matters you could have it stored in a totally sealed iron box. Not very useful when you come to want to spend it yourself! This brings us on to our second aspect:

Aspect Two

You want to be able to spend your money when you want to. This means you value the availability of it. Not only this, but you need it to be available in a usable format and timely manner, so if you are abroad you want the money to be in the correct currency when you come to spend it.

This also makes good sense. We have identified that in controlling our money we need to consider both restricting access to it (an appropriate degree of confidentiality) and ensuring this is balanced with a suitable degree of availability. However, there is another value that we should be concerned with, and to explain this we might consider the issue of foreign currency a little further.

Aspect Three

When collecting your currency, you do not — at least when first visiting a part of the world that is new to you — know what the money should look like or how you can be assured it is not fake. Most people are content to rely on the reputation of whatever company they choose to exchange their cash with. Nonetheless, we do value the fact that what we are being provided with is the real thing and not counterfeit. This is to say that we value the integrity of what we receive.

So with money we value keeping it out of the hands of others, having it accessible when we want it and in the format that we want it in, and that it is what it appears to be. When related to information integrity this can be summarised as 'complete and accurate'.

When referring to information this is the equivalent of valuing the information's confidentiality, availability and integrity; hence, when managing the security of information we need to consider these three aspects – much more than the layman's understanding of the word 'security'!

Organisations that wish to manage their information security arrangements typically introduce a set of policies, processes and working arrangements that help them exercise a degree of control to provide assurance with regard to these three aspects. This is generically described as an Information Security Management System (ISMS).

Who does it matter to?

Given the definition of information security as the preservation of the confidentiality, integrity and availability of information,[1] it is relatively easy to determine why this might be of importance to individuals, companies and public bodies.

It soon becomes obvious that it is not just the information that we need to be concerned with, but the storage, handling, moving and processing of it. When considering all of these arrangements it is relatively easy to conclude that every organisation should be concerned with their information security arrangements.

Individuals (members of the public or customers and staff) will want to know that information held about them is being managed and protected appropriately. Theft or fraud involving credit cards, credit ratings and people's very identities

[1] ISO/IEC 27000:2012 defines information security as the 'preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved'.

are well-publicised issues that mean information security is worthy of attention.

Companies will be driven by at least two factors: the requirements of their stakeholders and/or customers, and the need to remain competitive, protecting their IPR and reputation. Public-sector organisations have similar drivers to maintain a strong security stance and safeguard against security incidents.

In fact, many sectors have regulators that demand some suitable form of information management to be in place for anyone offering related services. Various governance regimes include requirements for information and information-processing arrangements, demanding that there are controls in place to enable directors to discharge their duties effectively. With high-profile governance failures in the headlines this is an area where pressure to comply will only grow.[2]

With the increasing trend towards relying on business partners for key services and processes, the need for some form of information security assurance is well recognised. Outsourcing and other contracts are now increasingly specifying compliance with some form of information governance regime as a mandatory requirement.[3]

The other key driver is the need to maintain a competitive edge. The obvious aims of not

[2] See *IT Governance: Guidelines for Directors* by Alan Calder for further information, available through *www.itgovernance.co.uk*.

[3] More on what assurances such schemes provide and on how to interpret any claims is provided in *Chapter 6*.

informing competitors of your costs, customers or trade secrets are concerns that fall within the remit of information security management, as are the less obvious benefits of effective information security such as improvements in customer service through appropriately managed databases (e.g. no longer sending mail shots to addresses that the client has told you they have moved from).

An effective information security management regime can provide an organisation with the foundations on which to build a knowledge management strategy and realise the true value of all the information that it holds.

The public sector has its own drivers, of course, including issues such as justice and national security, as well as the responsibility to become as effective and efficient as possible in conducting its work, in order to be able to truly demonstrate appropriate stewardship of public funds.

To all this should be added the obvious requirement that staff from any organisation will expect their personal information to be managed appropriately and their right to privacy respected.