

Data Security and the Privacy Act

You responsibly take steps to secure the access to your premises and you use passwords to secure access to your computers, but really, just how secure is your computer data?

Passwords are like old fashioned keys - if they fall into the wrong hands, they can be used by unauthorised people. These days, passwords are becoming more complex and being changed more often in an attempt to improve data security in theory, but the opposite effect is happening in practice. Many employees are writing down their new passwords because they are too hard to remember! This means anyone can find and use these passwords, especially another employee who wants to access records without being found out.

Then, there are the costs involved with administering an ever changing, complex password regime, the expansion of Help Desk services to cope with increasing password enquiries from staff, and the downtime of such staff who cannot log-on to their terminal until Help Desk issues and installs a replacement password for the one they forgot.

Next, there is the question of data security when your sensitive company records are transported outside of your premises. It is common for computer files to be taken to external meetings, presentations, on interstate or overseas trips, or just taken home to work on, as well as being regularly backed-up and stored off site as a prudent failsafe against a total systems failure. Such data can be transported on a Laptop, an external Hard Drive, computer disks, a memory stick or even emailed. In all these cases, the security for this transported data is likely to be even less than when it is contained within your office computer system. There have been numerous cases around the world where transported data has fallen into the wrong hands and ended up in the public domain. This could be a disaster for your organisation and your clients, and it could leave you exposed under the Privacy Act.

You may not have given all this much thought before, but are you aware of the obligations and penalties under the Privacy Act? Apart from your desire to keep your business records private and confidential, you also have a legal responsibility to adequately protect the personal information of your clients and staff from unauthorised access, modification and disclosure. If you check the Office of Privacy Commissioner's website, you will see a broad range of previous complaint case notes, summaries and determinations under the Privacy Act.

So, if you want data security that really does protect your computerised business records, both inside and outside of your premises, that enables you to comply with the Privacy Act, provides an accurate audit trail of access, and has the potential to save you money, then you should consider Biometric IT security. Start with a proven, cost effective and widely accepted Biometric signature, such as Fingerprints. Unlike passwords, Fingerprints are unique so only the authorised owner can gain access, they cannot be lost, stolen or passed on, and you do not need to worry about changing them. Modern Fingerprint sensors have a "liveness" test which is why they cannot be duplicated and why cutting off someone's authorised finger will not work.

Today, there is a large range of quality, latest generation Fingerprint IT devices available for businesses of all sizes. This includes single log-on or networked USB Fingerprint Readers for computer log-on &/or lock down, Fingerprint Flash Disks with up to 8GB memory which encrypt and protect data during transport, and Fingerprint Hard Drive enclosures into which you can place any sized HDD and it will encrypt and Fingerprint protect all your back-up files for safe storage

For more information on such products, contact Covetek Australasia on (02) 9404 8777 or web: www.covetek.com.au