Benscomputer.no-ip.org

Last October **Southampton University Hospital lost some 33,000 patient records (http://www.theregister.co.uk/2010/01/25/southampton_patient/)** when an *unencrypted* laptop was stolen from the back of a retina scan van. The laptop had been attached to the van using a cable, which was cut during the theft, but the only other security was password protection. The Data Protection watchdog - **The Information Commissioners Office (ICO) (http://www.ico.gov.uk/)** - has looked into the matter, and the chief of the hospital has promised to ensure that removable devices utilise encryption, and to ensure staff are trained adequately.

Although, in fairness, this loss happened some time ago, it does beg the question - why are organisations not using encryption?

Although they seem to get a lot more publicity, it is not just Government Agencies that are guilty of this, many companies in the Private sector are still not taking care of our personal data in quite the manner you would expect. Encryption solutions are widely available, ranging in price from **free (http://www.openpgp.org/)** to **thousands of pounds for a large company (http://www.gss.co.uk/products/index/Encryption_Solutions/)**.

So why is encryption not utilised more? The answer to this question is threefold at its most basic level;

1. Encryption is perceived as complicated
2. Password protection is seen as secure
3. Fear of data loss

Many of those in charge of a company, especially in the Small to Medium Business (SMB) arena, are not very IT Literate. They can't necessarily be blamed for this, they should be able to focus on running the business. However, it does cause problems when looking at security as a whole. Many users would not even know where to start if you asked them to gain access to a file without knowing the password to log onto Windows. Because it seems like such an insurmountable task, they assume that it is either impossible or at least technically complicated. Those with a little more IT literacy are aware that all you are likely to need to complete this task is a Linux live CD.

A similar situation arises when discussing the benefits of encryption, because the technology behind these solutions *is* quite complicated to the average person (try explaining how XOR works!), they can often assume that encrypting files will be too complicated for most of their staff. This is definitely true of some of the solutions available, but quickly ceases to be an issue when you examine solutions than utilise full disk encryption. There are a wide number of these solutions (again ranging in price from **free (http://www.truecrypt.org/)** to very expensive), but the most important thing is that they provide transparancy. If you can find and implement a solution that requires no user input (apart from a username and password to start the machine) you've probably found the perfect solution!

There's no reason for users to find encryption complicated, and if they do, they will probably try their best to avoid having to use it. If use of the encryption is made mandatory then a drop in productivity could occur as a result of an overcomplicated solution. Try to minimise this as far as possible.

Data loss can be very expensive for any business, so losing the encryption keys can be an understandable worry for many businessmen. If our data is encrypted and they key gets lost, how do we access those business critical documents? The answer is much the same as with an unencrypted disk, backup

backup backup! Add the keys to the businesses backup process (but ensure that they are securely stored). If a backup copy of the key is maintained than even if the user forgets/loses the key, the business will be able to access their documents.

There is an increased risk of data loss if users are able to arbitrarily create their own key pairs, so this should be restricted both technically and within the businesses IT Policy.

Additionally, you may wish to configure the users' e-mail clients to automatically encrypt e-mails sent to internal addresses and train the staff on how to encrypt e-mails for external users. This will quite possibly be the most complicated section of the changes as far as the users are concerned, so ensure the training is thorough and goes at their pace. You may also want to consider setting up an internal keyserver so that users can upload public keys for external contacts.

Whether you find an encryption solution or not, the most important things is *Data Protection Training*. Ensure the staff are aware of their responsibilities, and the consequences for both themselves and the business if a data leak did occur. Ask them to consider if they would be happy with the way data is handled if it was *their* personal data. Be open to suggestions about how things can be improved, the staff do their jobs everyday, and probably know the role far better than you.

These relatively simple steps are all that are needed to protect a businesses from the inevitable fallout after a data leak occurs. As with any solution, revise your policy and procedures regularly and train users to prevent confusion. Identify risks before they happen, plan for the worst case scenario and you should be able to help your business avoid making that call to the ICO.

So as an IT Technician, you should be proactively asking your customers whether they require an encryption solution, not every solution will fit every business so have evaluations of a number prepared. Offering to provide Data Protection training could also form a nice sideline that will be well appreciated in the SMB arena. If you are employed by a business, and believe that their encryption solution could be improved (or is simply non existant) proactively inform your employer of the possible solutions available, and the benefits therein.

If you are in the business of selling systems, this should simply consitute good customer service and is a reasonably easy up-sell to make, if you are employed by a company it is your responsibility to help a business thrive. Identifying and preventing the risk of a data leak is a very good place to start.

DISCLAIMER:

Note: all views expressed on this site are **my own**, and do not necessarily represent the views of my friends, family or employer.
