Encryption – key considerations

Encryption is one of the most talked about, but least understood, elements of the information security journey. There are a myriad of technology providers selling encryption solutions, which increases the complexity of implementing an appropriate solution.

Datashield's approach is to demystify the technology elements of the problem and then ally them with the other cornerstones of information security – people, physical security, third parties, and disposal of data to achieve a balanced solution.

So, let's look first at what you are required to do. You have a legal obligation to protect and secure data as a data controller. Allowing the transmission or storage of data which is not encrypted, wouldn't seem to fulfil that obligation given that the Information Commissioner's Office has made clear that password protection is not sufficient to constitute protection or security of data

Any portable devices or storage media provided to individuals for the purposes of working where they are remote, or cannot remotely connect to a secure network needs to be protected and secure, in other words, encrypted. Indeed there is a strong argument to say that even where users have to access secure networks remotely it is still more than likely that unencrypted sensitive data will be held on a local machine.

As part of a balanced approach you should consider how people work remotely. Take Outlook Web Access which is a great way of allowing access to email, calendar and so on to remote workers at minimal cost. In some cases this is the remote working solution, as opposed to a virtual private network (VPN). Users may access email via any browser so there is nothing to stop them saving data locally to unprotected machines. Consider the risk to your business of remote workers having significant amounts of your data saved locally on their PC which is accessed by children and family members. We have found sensitive data on unprotected home PCs which are connected to the internet using home broadband via unsecured routers.

In one case we located over 40 sensitive company documents on a home PC with no protection because they had been saved locally from a web based company email solution. The user had no idea how they would remove or clear down this data were they to dispose of this pc, meaning it had a high chance of being sold or disposed of with this sensitive data in place.

Where laptops and PCs are concerned you can use full disk encryption, where the user has to log on to the encryption system before the operating system will boot up. Alternatively you can encrypt only the files where sensitive data is held. This offers a lower degree of protection, as data is not always stored in one location by operating systems, and you will need to be sure that you have a process that stops data being stored in folder areas that are unencrypted.

There is also a choice between enterprise and standalone solutions. The latter are often low cost and easily available, but not all provide reliable methods of data recovery in the event of lost credentials, a major risk if servers are being encrypted.

Enterprise solutions bypass this by generating keys that can be used to recover data. This in itself presents challenges because the process around managing keys needs to be tightly controlled to avoid weak links in the security chain.

Enterprise solutions also provide many other features that may be useful to you. Non-repudiation, for example, means the technology will provide an audit trail of activity so users cannot deny that they created, deleted or amended a file. They also tend to encrypt to the highest current standards whereas other solutions may use less secure encryption methods. The difficulty is ensuring you implement a solution that is operable, yet provides the best protection at the right cost.

There are many “encrypted” USB drives available cheaply in the marketplace, but few would conform to FIPS140-2 standards, which is the relevant benchmark. In basic terms you get what you pay for, basic ones will encrypt the data and require password access whereas more complex variants provide the capability to remotely monitor devices, manage and audit content and remotely “kill” the device when it is lost. Cheaper devices will perform less well in terms of the speed at which data can be saved.

Another key area is mobile devices. Firstly if you don’t provide employees with phones or PDA devices it is likely that data is being stored outside your control. Mobile devices are very powerful these days with the capability to store word documents and spreadsheets they are the same as laptops, just smaller. There are a number of applications that can protect multiple operating systems such as Palm, Windows mobile etc. Enterprise solutions allow you to manage and clean these devices remotely.

Resolving these challenges is just the first part of the puzzle. You then need to give thought to how you protect data as it is in transit, i.e. ensuring the transmission method is secure and that the endpoints really are the computers you believe they are. After this you will want to ensure that any deletion of data is a secure process too. In many cases deleted data can be recovered from computer drives and there are a myriad of software products and destruction services to help you do this.

All in all the area of encryption is a minefield that you need to pick your way through carefully to avoid costly or impractical solutions, yet give an adequate level of protection. This is where a service like Datashield Professional can help. We consider your encryption needs as part of an overarching information security review which will help you ensure you are taking the right approach.