

Every day sees another headline that illustrates how data protection has been ignored resulting in vital data that has been exposed or lost. Yet it is common knowledge that enterprises have a vested interest, and a legal obligation to effectively protect data. Companies must understand, and account, for any mishaps and by merely adopting a security policy alone will only provide a false sense of data protection and potentially lead to the cost, embarrassment and humiliation of notifying customers, shareholders and competitors when data does go missing.

When you think of data security, it would be wrong to think of it as a static problem. Today's working lifestyle typically means data is mobile and carried across a multitude of devices including desktop PCs, laptops, notebooks, smartphones, PDAs, USB drives and CDs, and not just those meant to carry data - essentially any kind of endpoint computing device such as iPods, MP3 players and even digital cameras.

A better way to view data security is as a lifecycle, which can be broken down into four phases of data protection :

- **Detect:** You can't begin to protect data unless you can detect the devices where it is stored
- **Protect:** The protection of data (by encryption) has to be enforced
- **Manage:** Not only does data have to be protected, but also it will be necessary to provide management, audits, reports, etc to prove that protection was in place in the event of a theft
- **Support:** Users forget passwords; data has to be recovered from discarded media; etc.

Keeping these four principles in mind, this article provides a top ten tips to select a security solution to ensure you don't become tomorrow's big story :

Tip One : It's end to end

Don't fall into the trap of focusing on just one device or what appears to be the most obvious target such as your laptop population. Take a data centric view. Remember, it's about the data saved on a device and not what its saved on – keep in mind that the cost to replace a lost or stolen device is cheap, but brand loyalty and customer confidence are much, much harder to value or restore. Don't just buy laptop encryption and think you can sit back as you're covered – think of everywhere that data resides.

Tip Two : 'It's not my device' is no defence

If data is lost it doesn't matter what device it was on, data is data! Don't fall into the trap of assuming that the only devices you have to protect are the ones that the organisation owns. Referred to as the 'consumerisation of IT' by Gartner, the only device that an employee used (or even owned) 20 years ago was typically what the company had given them. Today, in comparison, everyone is using their own personal devices and hooking them up to the soft under belly of the corporate network. These are often used for legitimate reasons, but would you be able to identify if they weren't? And what happens if that personal device with corporate data on it is lost or stolen? Would you know? It's not enough to simply tell people not to do something, you have to make sure that they can't. Take an iPod as an example: It has a 60GB hard drive which can store huge



amounts of data. If corporate data is being transferred from the safe environment of the enterprise to any device such as an iPod, then it has to be protected.

This is where you might encounter another problem: Often, data protection solutions will encrypt files indiscriminately and this can be detrimental to some devices. (For instance, this approach will turn an iPod into an iBrick!) The best solution is one that recognises and accommodates different types of file according to where they came from, and doesn't just encrypt all files transferred indiscriminately.

Tip Three : What's out there

How can you protect something if you can't tell that it's there or in use? The answer, of course, is that you can't. The best solution will be able to detect devices trying to connect to the enterprise and sync up with corporate data. Once identified, depending on the policy that is set, it can either be blocked or protected.

Tip Four : It has to fit in

It's important to examine any solution's impact on existing operations within the enterprise. For instance, patch management is often done 'unattended', when the user is not present at the machine. The patching process frequently requires a re-boot, but what if the solution uses a pre-boot password (such as has to be used with a full disk encryption solution)? The only way around this in the full disk world is to temporarily suspend the pre-boot password, which means that the data is completely unprotected. The sensible way is to choose a solution which does not require any change to these operational processes, yet still provides full data protection. In other words, don't create a 'backdoor' security culture!

Tip Five : It's not an option

The underlying theme of data security regulation is that it must be "reasonable and appropriate". It should never be left up to the end user to make data secure – they don't have the time or the knowledge, and it certainly wouldn't be considered as "reasonable and appropriate" if the device, and the data it contained, was lost or stolen. It is imperative that this is controlled and managed centrally, wherever it resides, by qualified IT security staff – that way, in the event of a theft, they should be able to produce all the necessary reports and audits to prove that data was protected.

Tip Six : How secure is it really?

There are many who would argue that to be 100 per cent secure you must encrypt the entire disk. The reality is that this hides a huge weakness in that, if you encrypt the whole disk the same way, then if someone breaks in – or is already an insider – they have access to everything! To illustrate the point, take the typical case of an internal threat: The CFO of the company needs more memory or an upgrade; they hand their machine over to the relevant person who uses the admin code to unlock it; hey presto ... they have access to everything on the disk, including the CFO's highly confidential data! It is imperative that your data security solution includes the ability to uniquely protect individual users' data and separate the role of system administration and security administration, without interfering with the other operational processes (upgrades, patches, etc) that need to be done. And beware of solutions which offer this feature as a 'bolt-on' extra ... this typically means it's either poorly integrated, or it relies on another underlying mechanism (such as FDE) for security

Tip Seven : Prove it

It is not good enough to say you're protected, Corporate Governance requires you to prove it. When a device is lost or stolen then depending on local regulations the company has to decide if a "breach notification" needs to be issued, along with all the expense and embarrassment that goes with it. However, if there is a reasonable belief that the data was encrypted – and you can prove it – then you do not have to notify the affected individuals whose information has been lost as it is not at risk. By using a solution that includes a central management console, every machine that is protected reports back to say that it has received the latest instruction and confirms that it has been carried out, keeping all the proof centrally.

Tip Eight : Plan an escape route

When you start to roll out a solution you should never put yourself in the position of no return – this is another issue with full disk encryption because it's either 'on' or 'off' ... nothing in between. I know of an organisation who, when rolling out a competitors full disk encryption software, encountered a 30 per cent "brick rate" as it conflicted with a piece of software that hadn't initially been identified. An alternative would be a proof of concept but even this can be misleading as most laptop environments are uncontrolled and therefore you might not encounter an issue until you roll it out fully by which time it would be too late. The best option is a policy based solution which means it can be rolled out in stages. If it comes across a conflict then it can easily be stopped and taken back a step. In this manner you can gradually build it up bit by bit yet make sure you can recover gracefully from any problems.

Tip Nine : At what cost

Having recognised that protecting data is paramount, does it matter at what cost? Of course it does. The policies and technology used to secure the data need to ensure minimal impact on the quality of IT services - i.e. the impact on the usability of the device, the supportability from a central help desk (e.g. password recovery) and the impact on existing support and maintenance procedures. Some solutions require that all devices are brought into the IT department, are backed up and are then unusable for an extended period of time (e.g. half a day). Such a model is very expensive once you calculate the lost productivity for the user and the time for the IT staff.

A solution which protects all devices, and can be rolled out and maintained centrally without bringing in and locking down all devices for a period of time, will have a dramatically reduced TCO (total cost of ownership).

Tip Ten : Scalability

It's one thing to roll out to 100 devices and another completely to roll it out to 50,000. Make sure that the solution you select can be scaled up to accommodate the number of devices required, even if this figure is 50,000+.

In summary, when you're next evaluating your security requirements and considering any new technology, follow these ten tips and you will be able to navigate your way through to mobile data security.