An IT Manager's Insight Into Securing Removable Media
by Magnus Ahlberg - Managing Director of Pointsec Mobile Technologies - Tuesday, 9 November 2004.

When I last looked on the Internet to buy a USB memory stick, I found that for a few hundred pounds I could purchase a 4 gigabyte device the size of a pen. That's a lot of information you can now carry in the palm of your hand.

Thanks to their large capacities, portability, and simplicity, removable media have become one of the most popular types of storage devices around today. You've only to go down to one of the big computer shows to be offered a free memory stick as a stand give-away. If you take part in an IT training course, you might be given one with all your computer course notes stored on it.

If you're like me, the advantages of using a small memory stick, Compact Flash (CF) card, or the digital camera memory card are indeed enticing. Gone are the days when you have to lug your laptop around with you on every long journey or on spells away from the office. Just attach a USB stick to your key ring and you can carry all the documents you could ever need without that heavy, cumbersome laptop forever being in your shadow.

Removable media devices are a fantastic new addition to the constantly growing assortment of computer gadgetry that add convenience - even fun - to the way we work. But at what price? As removable media grow in popularity, more people are using them in the workplace to store corporate information. Documents, databases, graphics, music, even films and video can be tucked away on these highly portable devices. Yet the security implications and risks of removable media are considerable and need to be seriously assessed.

What happens, for example, if you lose your key ring which happens to have attached to it a USB token containing all your downloaded – and unprotected – corporate documents?
You're in luck, of course, if it only gets picked up by an inquisitive passer-by who, after reading it, finds your information is of little interest. But what happens if the information is accessed by a criminal, journalist or competitor? The entire contents of your PC could find its way into the public eye. Worse still, you can get held to ransom by the opportunist looking to bribe you so as not to expose the information that he/she has found on your company.

Perhaps most devastating of all, you could find the entire contents of your bank account emptied or even have your identity stolen. These

scenarios are very real and have the potential to be incredibly damaging.

As an IT administrator, if you don't have a handle on who is using removable media in your organisation, you have no idea who is downloading your intellectual property and other sensitive company information. You don't know where it is being taken, or what risks to which it is being exposed.

The harm to your business posed by information loss is not simply financial or operational. You must also consider the legal liabilities of information carried away on removable media. If a disgruntled employee decides to leak out information on your customers, you could find you are in for a very big libel suit as well as significant damage to your company's reputation.

Although tremendously useful, removable media devices, due to their small size, guises and uses, can be a serious security threat to any organisation. Here are a few hints and tips on balancing the benefits of these devices against the risks they pose:

Step One – **Security Policy** - Removable media devices are not toys. Decide how you as a company want to manage them. It would be naïve to think you could simply ban all removable media; however, you should introduce removable media into your Security Policy and make sure that everyone on your staff reads and signs the policy. Also, explain to your staff what actions will be taken if the policy is ignored.

Step Two – **Education** - Inform your employees about security and its implications. Explain why certain controls have to be put in place. Don't just impose those controls or users will ignore them.

Step Three – **Encryption** - Consider employing a mobile data protection product. Mandatory media encryption solutions are available that can be centrally controlled by the IT department. The best products are fast and transparent to the user, so as to not interfere with their real-time work. Such protection automatically encrypts all information loaded onto a USB token or other removable media. Access is granted only to the user who holds the password.

Step Four – **Control** - Implement device and executable control solutions that enable you to control exactly what devices can be connected to a system and what executable files can and cannot be run.

Step Five – **Audit and Measure** - Ensure that you carry out regular audits to find out who is using removable media

audits to find out who is using removable media.

In today's complex digital world, nothing about security can be guaranteed. But by following these few simple steps, you can mitigate your risk and show that you have taken adequate steps to do everything you can to protect the information that is being carried around on removable media devices. Once you do, you'll be able to sleep at night, safe in the knowledge that your company is not the next in line for public humiliation in the tabloids for allowing a leak of valuable information.