About the dangers of removable media

About the Dangers of removable Media

MAGNUS AHLBERG **The rise of the mobile data market has been rapid, lucrative and dangerous. Long gone are the days when you needed identical tape drives and software on both computers. The traditional floppy disk market and local tape markets were superseded by the super-floppy and zip drive. Now even they are disappearing as the mobile data storage market evolves.**

Thanks to their large capacities, portability and simplicity removable media have become one of the most popular types of storage devices around today. You have 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. They are so cheap, it is the obvious way to store information, business proposals, accounts, client's details and marketing plans.

The arrival of the MP3 music player has had a significant impact on the market. While Apple sees music as the only reason for owning an iPod, their competitors have simply created large USB stores with some built in music software. An increasing number of people now view the MP3 player as both a data and entertainment tool. The danger here is that as an entertainment device it falls below the radar and with storage capacities set to exceed 80 GBytes by the end of 2005, it is a serious threat to data protection.

10 Things you should know about this Market

1. The first Compact Flash Drives began to appear in quantity five years ago and started at 8 MBytes. By 2004, Lexar had released an 8 GBytes device aimed predominately at the professional photo-market.
2. USB Pen Drives are now often hidden inside pens making them very difficult to detect by security teams.
3. Seagate now ships a proper, very small form factor 5 GBytes USB disk drive. It is less than half the size of a Yo-Yo and features a real disk drive spinning at 3600 rpm.
4. 4 GBytes USB pen drives are expected to reach capacities of over 8 GBytes by mid 2005.
5. New mobile phones can use memory cards holding in excess of 1 GByte.
6. Research in 2004 suggested that a modern office worker carrying an MP3 device and a mobile phone would be capable of storing over 20 GBytes of data.
7. MP3 and mobile video player company Archos will soon launch a 100 GBytes device.
8. The new 1-inch hard disks are expected to reach 100 GBytes within twelve months.

The MP3 music player has had a significant impact on the market.

9. Blocking the USB port would prevent all devices from working and with operating systems like Windows XP, is easy to circumvent.
10. IDC predicts that the sale of very small hard disks will explode from less than 18 m in 2004 to over 100 m in 2008. Most of those will be in portable devices that could be carried into offices.

If this does not scare you then you clearly are not responsible for looking after corporate security.

Some Facts about Corporate Data

1. The average word processing file is 3 pages in length and between 25 and 30 k. That means that a 20 GBytes MP3 player could hold over 750 000 documents.
2. The majority of corporate networks do not audit what kind of data a user copies to a local machine or attached device.
3. New compliance legislation means that you must develop a policy for the use of devices or risk being fined by regulators.
4. 99% of users who use mobile devices to transfer data use no encryption to protect their contents.

Think about how easy it would be to remove your corporate data. During the 1980s the fear was that people would be able to save the customer or company price lists onto a floppy disk and take it to their next employer. Today, they can not only take that information but also your entire customer database showing purchasing prices and history on a single device.

The advent of fast Internet access in the office meant that employees used the company network to download files. Increasingly, that has meant people pulling down illegal content as well as installing peer-to-peer (P2P) networks on their desktop computer. With P2P installed, they can move files between the office and home on CD, DVD or other removable media. The danger to the corporate network is that file sharing through P2P exposes the company internal structure.

Preventing people bringing devices and media into the office is an extremely difficult problem. Look at the physical size of much of this media and it is easily missed in a pocket, briefcase or handbag. Short of instituting an invasive and very workforce unfriendly search policy, keeping devices out of the company is virtually impossible.

The solution then, appears to be one of management. The first step here is to decide on what you can and cannot enforce. Remarkably, few companies actually realise how limited their powers actually are, especially with respect to current privacy and human rights legislation.

For example, preventing employees from bringing their MP3 player to work and then using it during lunchtime would require draconian terms of employment that are almost certainly illegal. Companies that have tried similar experiments with regard to camera phones have found it hard to police and enforce.

What can you do?

Ensure that all members of staff are aware that their employment does not allow the connection of non-company devices to their computers or other peripherals. This means banning people from downloading their photos to that nice colour printer. No swapping music with the person who sits next to you if that means connecting to the computer and using it as a transfer point.

Administrators need to create security solutions that log the amount of data that a user downloads. It is already acceptable to search an employee's hard disk for illegal files but few companies do this. Nightly sweeps of hardware to find MP3, WMA, JPG and other file extensions would seem a simple thing. Unfortunately, all of these formats have legitimate work uses and are often used by software packages for saving business files.

If you are to allow data to be transferred over removable media then you should consider how to secure it. There are several vendors with encryption solutions in the market. All of them have different advantages, but whatever you choose should have a minimum set of features.

1. Work with policy files to allow data to be locked after a given number of password attempts.
2. Have a mechanism so that data can be encrypted once and then accessed where required without having to install software on the receiving computer.
3. Be backed by an administration program that would allow for the recovery of lost passwords.
4. Will work on a range of devices and removable media.
5. Be simple to use, implement and manage.

The latter is all too often overlooked when deploying security solutions. There is a belief that security means complex, it does not. To ensure that people use a solution it must be simple, effective and deal with all situations. If you have to give encrypted files to someone who needs a copy of the software, then it becomes a case of either give them a licence for the software or do not encrypt. Many people will opt for the latter.

Files need to be self contained as an executable where the level of encryption is still high enough to thwart all but the most extensive brute force attack. There are products that fall into this category and they are worth finding and deploying in order to minimise the risks. One possible solution is to ensure that you encrypt everything that is downloaded from a computer onto any removable media.

Your Corporate Data has never been so insecure

The ease with which this can now be removed from the office surpasses anything in history. There are approaches that you can use but they must encompass protection of content, and system management simply banning devices will not work.

Remember, we are now in a world where almost every month a new piece of regulation over data protection and access appears. If you do not sort this out now, the regulator will simply fine you extensive amounts of money and you will still have the problem. ■

Magnus Ahlberg, Managing Director of Pointsec
www.pointsec.com