

Top 20 *Essential* Steps For Securing Your Confidential Data

The most common security flaws that many businesses make that puts their data at risk...and how to avoid a **DATA-LOSS DISASTER!**

In this report you will find some useful strategies that you can put in place to immediately reduce the risk of the loss, or theft of your personal, or company's confidential information.

Never before have the subjects of data-loss and ID theft been so much in the spotlight. Whether it be confidential company information on research and development, customer or supplier details, patient files or personal finance info; there is a huge and growing market for each and every piece of lost or stolen data for both legitimate and illegal use. The financial rewards can be huge.

Reputations can be lost, fines levied and now perhaps soon, jail sentences too, for anyone found to be negligent in a data-loss or data theft situation.

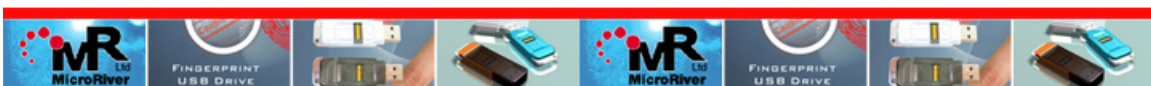
With MP's now calling for the criminalisation of negligent data loss, it seems only a matter of time.

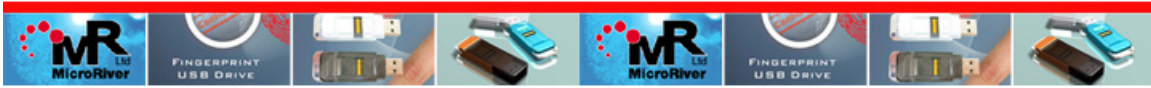
This report will give you a guide to the steps you should consider to protect yourself or your company from the loss or theft of your data. Some of the areas outlined may seem very simple, but you would be surprised at how many companies do not have them in place today.

Let's begin with The Basics

Physical Security

Have a look at your office today. Could someone simply walk on in? If so, could they get past your reception





unchallenged? Are you holding any critical files on the receptionists PC? Do you have any backup drives, removable drives or other laptops etc at, or near to, the reception desk?

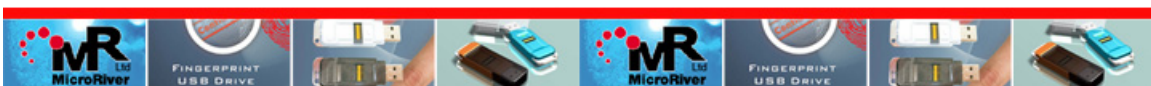
Cont

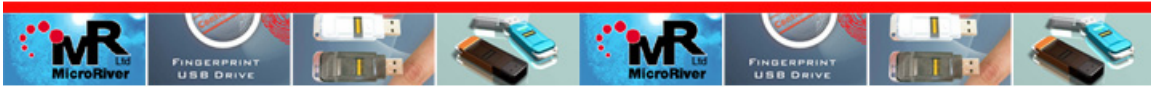
Recommendations:

- * Secure your entrance / reception to ensure no-one can get past this point without a pass, a key or an escort by a staff member. If this is not possible, lock down each and every desktop PC, Laptop and portable storage device in the office using the methods below.
- * Secure the computer at reception using brackets and screws to ensure no-one can just walk in and take this machine away. (Sure it's obvious but you'd be surprised)
- * Move any backup drives to a secure area of the office or into a locked communications cupboard or room.
- * Use a "cable lock" to secure your laptop/s which are sitting at desks or workstations - this won't stop organised crime as a decent set of cable cutters will easily sever the cable but will stop the opportunistic thief.
- * Put all laptops out of sight when not in use (eg in a locked drawer)
- * Ensure all staff removes any company information from unsecured USB keys (memory sticks) as these are easy pickings for anyone wanting to get to important information. All company information should be stored on secure USB sticks which require fingerprint authentication before allowing access to any of these types of files. (more info on USB sticks further on)

Password Security

Amazingly, many people find it an inconvenience to enter a password to access their computers, but I highly recommend you adopt this practice. The password is your first line of





defence and this feature should be enabled on all computers within your organisation. The password should be required when you turn the machine on, and should also be enabled in the screensaver mode.

Recommendations:

* Enable password feature on computer start-up. You can do this by going to the "start menu", then selecting "control panel", then "user accounts" (works with most windows based machines).

Cont

* Enable password prompting on your screensaver and have this activate within 10 minutes of the computer being idle (preferably shorter if you want tighter security) to ensure no unauthorised person/s can access your computer if you're away from your desk for a period of time.

You can enable this by right clicking on your desktop, then choose "properties", then the "screensaver tab", then tick the "On resume password protect" box (works with most windows based machines)

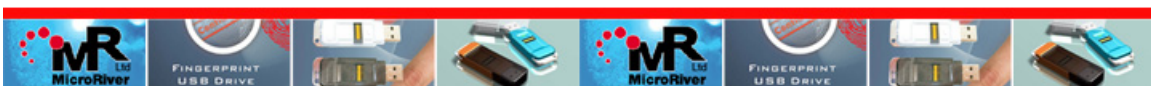
* Don't use passwords like your company name, or "password", "admin" or "administrator". That's how the billion-dollar, US pentagon's defence system computer was compromised by a young hacker from the UK who wanted to find out about UFO's. Bizarre but true!

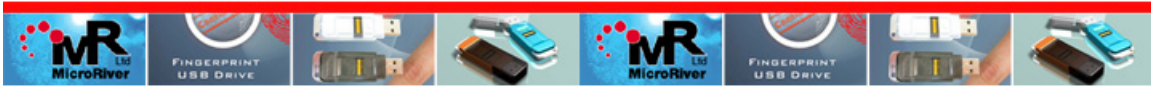
Keeping Your Data Secure

Let's look at Remote Access

To date, we have used various methods to protect our company or personal data. However, because of the increased risks we now face, it seems that these are no longer sufficient in their present level.

Today, firewalls and access controls are common place. Networks can be protected by using multiple layers of firewalls. However, the computers used by staff at home to communicate with the office and access the company data may





not even have basic firewall protection. Even if it does, it may not be updated regularly. And of course, if access control is inadequate, firewalls will not stop unauthorised persons reading or copying the data.

Recommendations:

- * Review all remote access use and determine if any access from outside the workplace is not really necessary. It is essential that you review this regularly. Ensure all remote access computers have adequate security and protection installed and enabled.
- * It is also essential that it is impressed upon all staff that data protection is the responsibility of everyone in an organisation and not just the IT team.

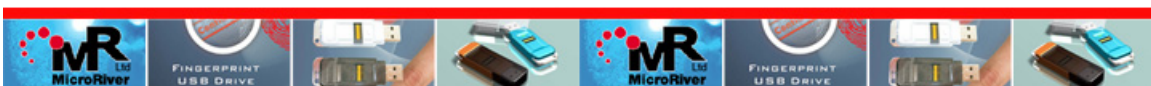
Cont

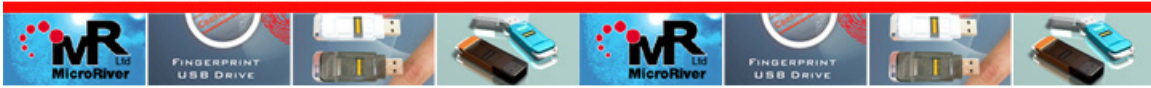
- * Carry out a risk assesment and draw-up an action plan to protect against potential loss or theft. This should be communicated to all staff members and discussion encouraged. Clear lines must be drawn on the subject of what is acceptable to the organisation regarding remote, laptop and USB use and what is deemed to be too risky.
- * The same goes for mobile devices such as PDA's and Blackberry's. The very mobility of these devices that makes them so handy, also means that they are vulnerable to accidental loss or theft.

Terminated access rights

One strong area of risk is the failure to restrict unauthorised access by staff that has no valid reason to have access rights. This may seem obvious but it is nevertheless a major cause of data leakage. A common security failing in many large companies is to terminate the access rights to departing users at the last place that he or she was located, but neglecting to terminate access rights at their previous workstation or location.

Recommendation:





* Review unauthorised access list and terminate access rights to departed user's at all previous workstations.

Email encryption

Email is a key area of risk for many companies and organisations. Sending unencrypted e-mail of a sensitive nature is like sending a postcard in the mail. It can be intercepted, read and then passed-on without sender or recipient being any the wiser. There are actually companies whose sole business is to do this; scanning for sensitive information with spyware, using keywords and phrases for other interested businesses or individuals.

Recommendations:

* Always encrypt confidential e-mails. This enables you to secure the content and restrict access to read the content to the named recipient only. Encryption specialists Ultimaco has a system that enables e-mail to be sent as encrypted PDF documents.

These are readable only when the correct password is entered by the intended recipient.

Cont

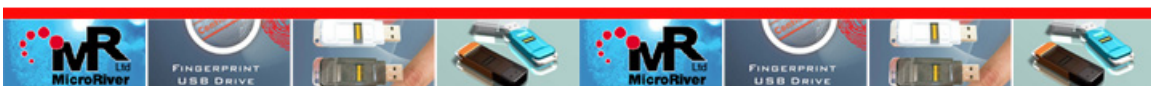
If you send confidential information by e-mail, then this is definitely worth adding to your security measures if you have not already done so.

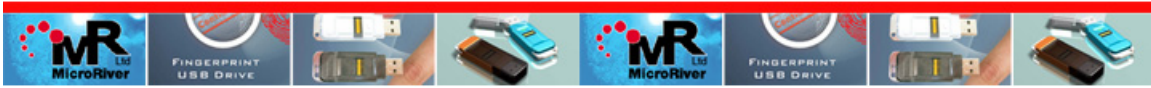
It is worth adding that not all encrypted e-mail necessarily has to be outward bound from the workplace. Encryption is also a good idea for confidential internal e-mail too. The curiosity of some employees can often get the better of them.

Unsecured Wireless Access

Many people are still not aware of this but it is like an open invitation to come and have a look through your hard drives.

Are you currently running a wireless network? If so, do you really need it? In other words, is there a network point close by which could be used instead?





Wireless networks are your weakest point of access. If you have, or are considering setting up your own wireless network, be aware that the default set-up in most wireless routers configures the connection with absolutely no security! This means anyone within range can connect to and use your connection to the internet, or worse, access your confidential files!

Did you know that in many cities in the UK you will find chalk markings on the footpaths outside buildings? These markings tell other like-minded people what wireless networks are available and what security (if any) is enabled - so that person sitting on that park bench with their laptop or in that car outside your office could be accessing your wireless network right now!

If you must run a wireless network, be sure to turn on encryption and go the next step by also setting a list of approved devices to connect to your network.

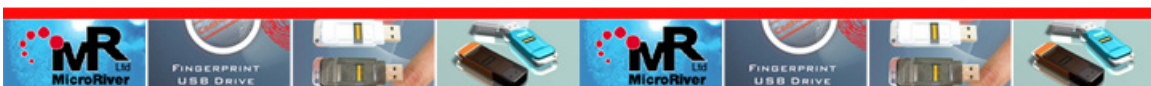
Recommendations:

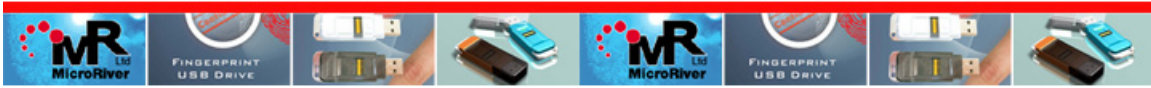
- * Turn off wireless networks if they are not critical to your business.
- * Turn on encryption if you must use a wireless network.
- * Lock down your wireless network to fixed MAC addresses.

Cont

Each computer has a unique MAC address; it's like its DNA. These are hard coded into the machines and are difficult (but not impossible) to replicate. Once the wireless connection is established, you can instruct most wireless routers to restrict access to only those chosen MAC addresses.

This can be a little annoying if you regularly have new users wanting to connect to your wireless network, but is worth the investment in time. Once setup, It is also recommended you turn off the "broadcast" option in your wireless router - this will ensure that your network is not "advertised" to anyone else within wireless range.





According to the DTI Information Security Breaches Survey 2006, the vast majority of companies still rely on weak, static password security. It is worth bearing in mind that the same survey found that 60 percent of companies that allow remote access do not encrypt transmissions and as a result are more likely to have their networks penetrated.

TJX – parent company of TK Maxx had 45 Million customer records hacked in this way; even though WEP had been activated. This was the biggest loss of credit card data in history. (WEP is the wireless security standard. Currently the world record for cracking WEP, set in April 2007, stands at 3 seconds)

USB Keys (Memory Sticks)

Last, but definitely not least, let's look at the USB key or flash drive.

These are a fantastic device as they are portable, can hold ever-increasing amounts of information and are the quick and easy way to store all of your important files in a neat little package. Most people use these to backup important documents and files.

Many people transfer their current projects onto it, so they can take it out of the office to work on at home. Others keep all of their personal and secret information on them, like their documents, personal photos and emails or latest project etc.

Although very convenient, the majority of these devices are NOT SECURE in any way.

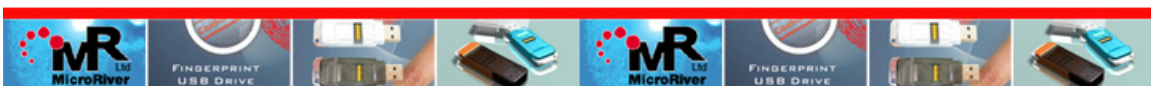
Should you drop this in the street, or have it stolen from your office, home, car or handbag, all of your information will be instantly available to the finder/thief upon insertion in their computer.

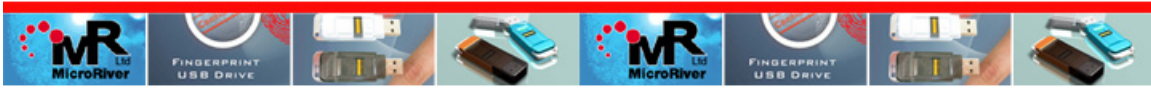
Cont

What will they find out about you, your business, your clients or your next product launch?

You could be handing them the sensitive, personal details of hundreds, thousands or even tens of thousands of customers or clients. Maybe confidential business information!

Unsecured USB drives can be a real weak point. As they are so small, they can easily be lost or stolen. They can easily





be concealed and carried in and out of areas that they have no need to be in, and sensitive information and data can be downloaded to them quickly and discreetly. Companies and organisations should use strong, two-step authentication devices. This involves a password in conjunction with another method of authentication, such as a Biometric/Unique Fingerprint access security.

Recommendations:

- * Restrict all USB drive use to only company approved devices. Use only USB's that have both Biometric and password security.
- * Block all ports to unauthorised USB's.

All unsecured USB keys should be banned immediately if you are in any way serious about data security!

According to the DTI Information Security Breaches Survey 2006, only one company in seven actually encrypts data on hard disks. Recently a laptop containing salary details, addresses, dates of birth, national insurance numbers and phone numbers of around 26,000 employees went "missing" from a printing firm which was writing to M&S workers about pension changes. Another laptop theft, led to the sensitive info of more than 16,000 council workers at Worcestershire County Council being put at risk.

Laptop theft is BIG Business. It is a huge and growing problem.

In 2006, the Metropolitan Police Force had 6,576 laptops lost or stolen.

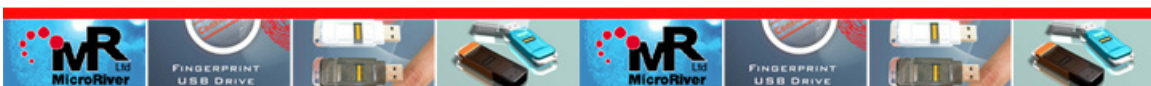
Little wonder then, that 15 police forces across the UK now use the revolutionary new iSecure Biometric USB drives from MicroRiver. Not only is the data they carry now secure, but the need to carry laptops from place to place is no longer necessary.

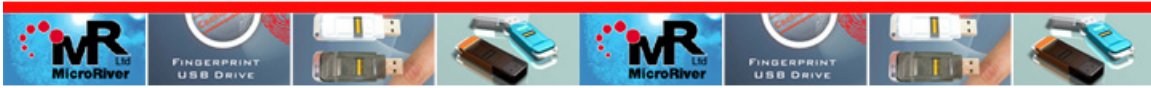
Gartner research found that 22 % of Flash drives are sold to enterprises. About 80 to 90 per cent of those are not encrypted and organisations know there is a problem with that. iSecure Biometric USB drives could stop a potential disaster right now! Why take the whole laptop out of the workplace when you could just take the data on the USB drive - complete with applications if needed, safe in the knowledge that the data is secure!

Cont

Just look at these cutting-edge security features:

Biometric (Fingerprint) Data Protection.





Protect your data with your Fingerprints and a backup password. Simple and safe.

Safe Login / Password Manager, Website Auto login.

Save website passwords and logins with just one click. Access your favourite websites faster and have your passwords with you on your portable device.

Outlook® synchronization

Keep your Outlook profiles synchronized between different PCs. Always have your Outlook up-to-date whether at home or work. When you are travelling, the convenient Portable Outlook functionality allows you to access all your Outlook data on a remote PC just like it would be your own.

Portable Microsoft Outlook®

Have all your e-mails and contacts with you and use them on computers that have Microsoft Outlook installed.

Portable Microsoft Outlook Express®

Manage your contacts and emails while on the move. You can do this easily on computers which have Outlook Express® installed.

Favourites synchronization (Internet Explorer & Firefox)

Keep all your links with you and access them from any computer.

No Trace Browsing with Internet Explorer & Firefox

With No Trace Browsing you can safely browse the Internet from any PC without leaving any traces that could reveal what information you accessed or what websites you viewed on the Internet.

Desktop, Folder to Folder and My Documents synchronization.

Instant synchronisation of your documents, files and folders. With just couple of clicks you can carry all the data files you need, whenever you like.

Data Compression

Ever wished your USB drive had some extra megabytes? Carry it Easy +Plus Bio™ lets you compress your data on the fly and save space on your drives.

USB Drive Lost & Found™

Let the finder(s) know who you are but don't let them see what's on your Flash Drive.

USB Drive information

You're in control! It's your drive! Find out all you might want to know about your USB Drive.

End

Copyright David Ewen Marketing 2008 DavidEwen.co.uk

