

FEATURE

PROTECTING MOBILE AND NETWORK DATA

By Ian Kilpatrick, chairman of Wick Hill Group, specialists in IT security

Summary:

- * Company data used to be regarded as very important but has now lost its value
- * Mobile data storage is now cheap and widely used
- * Mobile devices are continually lost, creating a security risk
- * Companies need to better manage data on the network, in transit and remotely
- * Recommendations on how to manage data more securely



- restricting and managing downloads onto devices such as USBs
- encrypting data on mobile devices
- managing and authenticating network access
- training staff
- monitoring network usage to pick up non-compliant staff behaviour
- proving that you care about data security

Company data has lost its mystique. It used to be thought of as an incredibly important asset. Now, with mobility, universal 24x7 access and an 'always on' approach, data isn't seen to have the value it once had.

Alongside that, mobile data storage has mushroomed. When consumers can now buy (and lose) 2GB USB flash drives for under £5 and ½ terabyte drives for £200, data is perceived as a commodity.

Mobile devices are continually lost. In airports, Heathrow tops the EMEA list at 900 lost laptops per week, followed by Schiphol with 750 and Charles de Gaulle with 733.

A Credant Technologies report found that 60,000 devices were left in London taxis in a 6 month period in 2008. <http://news.bbc.co.uk/1/hi/technology/7620569.stm> 60,000

The 'It will never happen to me' approach is clearly flawed. And just telling people to take care of data obviously isn't working.

Companies need to manage their own data inside the network, in transit (on CDs, USB flash drives, etc.) and remotely (with mobile workers, day extenders, etc.). It is clear that, even excluding deliberate misuse and data theft, data will be lost.

The huge number of reported embarrassing incidents of data loss is just the tip of the iceberg and insurers are now specifically limiting publicity on any data leaks/data loss, to minimise their liability.

Keeping data secure

However, there are steps you can take to make both mobile and network data more secure.

** Restrict and manage data downloads onto devices such as USB flash drives.*

USB flash drives are an incredibly easy way of moving data from one computer to another, even very large amounts of data. But they are so easy to use, so easily transportable and so easy to lose that they present a serious security risk.

There's also the risk of staff using USB sticks to download data which they shouldn't or inserting unauthorised flash drives onto the network, which may contain viruses or spyware. There's also the risk of visitors using flash drives on the network or connecting laptops.

Companies need to have and enforce rules in their security policies to cover the use of flash drives and other mobile devices which can be connected to the network and taken away from the office. Downloading data, in particular onto flash drives, should be restricted and their use actively managed.

There are a number of solutions available that can manage this, from mainstream security companies such as Check Point and Nortel, and also from many niche suppliers

** Encrypt data on mobile devices such as laptops and USB flash drives*

Where it's necessary to use flash drives and other mobile devices such as laptops or PDAs, then the rule should be to encrypt everything. Then, if something is lost, which seems inevitable, the data is protected.

On laptops, full disk encryption is probably the best route to provide proper protection. This should be coupled, of course, with suitable back-up for users who may forget their passwords.

** Manage and authenticate network access*

One of the most basic security functions in any organisation is proper access control. This will prevent unauthorised users accessing confidential information and using unauthorised flash drives or other mobile devices on the network, whether in the office or remotely.

In today's computing environment traditional, single passwords, on the whole, are no longer suitable and strong two-factor authentication should be used. This involves something you know (a PIN number) and something you have (a hard or soft token, for example), which gives a changing one time password (OTP).

You can also enforce encrypted VPN access to the corporate network for laptops, remote users and day extenders, which provides additional security.

** Train staff*

Training is absolutely critical in protecting data both in and out of the office. However, whatever you do, there will always be those people who want to do things differently to your stated security policies. No matter what you say about the importance of the correct way to protect data when using flash drives, laptops and other mobile media, there will be those who feel that the security procedures are just there to stop them doing their jobs. Or those who simply feel they know better.

One way of addressing this is to get department heads on board to stress the value of data to the company and to their department in particular, and the need to protect it. Without departmental and company-wide buy-in, policies are destined to struggle or fail.

** Monitor network usage to pick up non-compliant behaviour*

The way to reinforce policies is, of course, to overtly care about them - typically through monitoring and reporting. A range of network tracking tools from companies such as ArcSight and LogLogic is available, which will monitor and record everything that happens on the network. Such tools will tell you if someone is trying to use an unauthorised USB or connect up other unauthorised devices, such as their ipod, to your network.

Monitoring tools can also identify whether someone is attempting to carry out unauthorised data access and activity on your database. This way you can pick up questionable behaviour before any data is potentially stolen.

** Prove that you care*

Act on the information you pick up from your network monitoring tools. If someone is trying to use an unauthorised USB on the network, then make the person and their manager aware that you know what they're doing. Companies must decide on their own disciplinary procedures when this happens, but at least people know that there is active monitoring, if they breach security policies.

If you don't identify and act on breaches of your policies, then the breaches can escalate. This phenomenon is well known from the accounting world. Someone may start out with a minor breach, even something they do by mistake. If it is undetected and not acted upon, it can lead to a situation where people may decide to take the customer database with them when they leave, because they think no-one will ever do anything about it.

** Encrypt data on PCs in the network*

Research has consistently shown that internal security is just as much a problem as external security. Staff are at least as likely to steal data as external hackers. So it makes good sense to encrypt critical data on your network.

Bio Ian Kilpatrick

Ian Kilpatrick is chairman of value added distributor Wick Hill Group plc, specialists in secure infrastructure solutions. Kilpatrick has been involved with the Group for more than 30 years. Wick Hill is an international organisation supplying SMEs and most of the Times Top 1000 companies through a value-added network of accredited resellers.

Kilpatrick has an in-depth experience of computing with a strong vision of the future in IT. He looks at computing from a business point-of-view and his approach reflects his philosophy that business benefits and ease-of-use are the key factors in IT, rather than just technology. He has authored numerous articles and publications, as well as being a regular speaker at conferences, exhibitions and seminars.

ENDS

For further press information, please contact Annabelle Brown on 01326 212130, email abpublicrelations@btinternet.com. For reader queries, please contact Wick Hill on 01483 227600, web www.wickhill.com. For pic of Ian Kilpatrick, please contact Annabelle Brown or download from <http://www.wickhill.com/company/press/pictures.php>