The why and how of setting up a mobile security policy

The proliferation of laptops, PDAs, smartphones and USB sticks means that corporate data is no longer confined to the office. Without a joined-up policy on mobile security, protecting and keeping track of it becomes impossible.

For the staff member who needs to work at home, or at other remote locations such as customer sites, transporting data out of the office has never been easier. Just plug a PDA, smartphone or USB stick into a desktop PC and drag the required files onto it. If none of these devices is to hand, a digital camera or an MP3 player will suffice. Windows will instantly recognise them, without the need to install any drivers, so users don't even need administrative privileges on the desktop in order to do this.

If the staff member has a laptop PC, things are even easier. Just plug the machine into the company's network and copy the required files directly from the server.

But all this convenience comes at a sometimes hidden but high price. Without the necessary procedures and technical restrictions in place, companies can easily lose track of their sensitive data.

- Just how many files have been copied in this way?
- Where are they all now?
- Are legitimate users working with outdated versions because they have neglected to copy the most recent ones?
- Are dishonest employees copying files that they don't need?
- How many former employees, now working for your competitors, still have your data in their possession?
- How often do staff copy a file to their spyware-infested family PC to work on at home during the weekend before unwittingly bringing the infected version back to the office on Monday morning?

The Solution

What's needed is a mobile security solution which the user isn't aware of, so it's easy to use, totally transparent and doesn't effect the performance of the device in anyway. It needs to be configured so that its use is mandatory by all users and on all mobile devices. In addition, it should include key recovery facilities so that any file can be recovered by designated administrators in an emergency without the co-operation of the user who created it. Most importantly, the technology should be vendor-neutral, capable of working on every mobile device from USB stick, iPod, camera and smartphone to Windows laptops.

If you have always assumed that such products don't yet exist, prepare to be surprised. They do exist, and have done for a few years, albeit as part of a market that has only recently reached maturity. The whole sector is now growing rapidly, as more and more companies accept that they can't stand idly by and watch their data spread itself far and wide. If you've been avoiding the problem, you really shouldn't continue to do so. Now is the time to roll out a mobile security policy.

Choosing a Strategy

One crucial question that many companies consider when evaluating mobile security products is whether to go for the “big-bang” approach and roll it out to every mobile machine from the start, or whether to start with just a few devices and complete the rollout over an extended period. We would always suggest you rollout from the start as staggering the process is just asking for trouble. If a machine gets stolen or lost, you can just bet that it will be one which hasn’t been protected yet.

Whichever supplier you decide to go for, choose carefully. If there’s an offer of some reference sites, contact those references and ask questions. If no reference sites are offered, ask why. Look, too, for industry certifications within your business sector, and for an organisation that can support you 24 x 7, just in case problems do arise. In short, go with an established player and a market leader, so that you can have confidence that the product you choose will continue to be supported and developed in the future.

Top Tips for an Effective Mobile Security Rollout

1. Roll it out to all devices from the start, rather than just those which you think might be the most deserving. It will save you time and money in the long run.

2. Choose an established vendor which offers 24x7 support, satisfactory reference sites, and relevant certifications.

3. Look at the total cost of ownership, including ongoing support and upgrades, rather than just the up-front licence costs.

4. Ensure that the product supports all of the hardware platforms that you use, and which you intend to use in the future.

5. The recently-published DTI survey http://www.dti.gov.uk/files/file28343.pdf into security breaches in the UK will help you to convince senior managers that mobile security is a major risk that must be addressed sooner rather than later.