How Secure is Your Data?

Protecting Sensitive Data on a laptop or other personal computer is a vital part of any computing environment. However, no user wants to be burdened with unnecessarily complex steps or configurations and the same is true for the busy IT support department. It is therefore worth considering alternate solutions for securing sensitive data. There are a good selection of solutions to the problem of protecting the data on a hard disk drive (HDD) all of which involve the encryption of that data.

Software Encryption Does not Make the Grade

While software encryption is more secure than no encryption at all, it does have its limitations. A software encryption solution can protect a partition or an entire hard drive. The solution may only be compatible with select operating systems and may interfere with some software applications. System performance will also be affected by software encryption running in the background and will thus affect the performance of other applications. Such a solution is seldom transparent to the user and an attacker may be able to disable the encryption application. When a partition of a hard drive is protected using a software encryption solution, the unencrypted information may be stored in plain text elsewhere on the hard drive. In addition, the encryption key may also be stored in plain text on the hard drive. A hard drive or any other medium protected by a software encryption solution presents administrative problems. When a drive is imaged for backup purposes, the encrypted information needs to be decrypted to plain text – a time consuming process – or the encryption key needs to be copied as part of the image thus compromising the encryption solution. Software encryption can protect sensitive data but it increases system administration effort and may conflict with other applications. Due to the above limitations, a better type of encryption is available namely hardware encryption.

The Power of Hardware Encryption

A hardware encryption solution performs the encryption function within the hardware of the computer components making it completely transparent to the user. This kind of encryption does not depend on the operating system or any other applications and has no noticeable affect on system performance. For a fully encrypted hard disk drive, all information that resides on it is protected. A rogue user who cannot authenticate himself to the drive cannot image a device with hardware encryption. This prevents a brute force attack and other hacking techniques from being applied to the encrypted device and also makes imaging for backup and recovery purposes more straight-forward.

A hardware encrypted device does not rely on any software applications, patches or license agreements; this can save considerable administrative time and financial resources over the long term. In a December, 2004 article in Electronic Business magazine, it was reported that analyst firm IDC has forecast that by

2007, 80 percent of computer security will be hardware, rather than software, based.

How safe is the data?

Today data recovery techniques are increasingly sophisticated and all data can be removed from a regular HDD with ease leaving software products exposed to attack. Rules imposed by encryption software while operating, such as ‘three attempts and you’re out’, are readily circumvented by copying the software and data on the disk and attacking the copies. This is not possible with a hardware encrypted HDD because users are authenticated by systems separate from the enclosed HDD itself and encryption keys are not stored on the disk.

The Right Solution

The Classified PC line of mobile and desktop computers use a fully encrypted hard disk drive and an in-line on the-fly hardware encryptor packaged within a strong tamper resistant and tamper evident case. All data held within a Classified PC system is fully encrypted with user access under password control. The password is entered at boot up, prior to initiating the operating system, preventing attack from any malicious code introduced onto the hard disk drive.

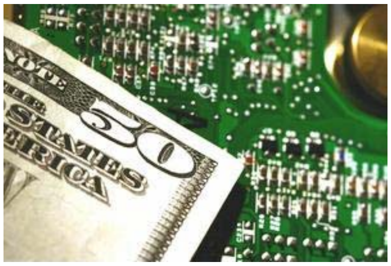
Support and Integration Issues

For a software HDD encryption solution substantially more set-up is required including both the installation and the configuring of the encryption software after loading the user’s data image. Using a system with a hardware encrypted drive requires only the imaging of the drive and loading the user’s data. Simple and straightforward.

It is common practice for today’s operating systems to be updated regularly and each time this happens the changes made may affect the HDD encryption software. IT Support must be engaged in this process to ensure the smooth roll-out of upgrades and so implies the funding of a suitable software support contract for the life of the product. Fortunately a hardware encrypted HDD solution suffers neither of these drawbacks saving on time, effort and ongoing annual software maintenance charges.

In Conclusion

To achieve the levels of security needed to meet today’s distributed and mobile PC data management requirements, a hardware-based solution is the perfect complement or replacement to the security protection offered by software. Hardware’s rigidity or inflexibility makes it more difficult to change than software and it is thus an excellent platform for increased security in situations where protecting sensitive data is of paramount importance.



The up-front cost of a software HDD encryption product may seem attractive at first. However, once the additional costs of deployment and maintenance are factored in to the typical product life cycle of over five years, the additional initial cost of a hardware encrypted HDD system is easily justified by the savings made.

Therefore, hardware encrypted solutions, like a Classified PC, can be presented as a more attractive option than their software competitors in terms of security, usability, project management and cost.

iWave, LLC
Secure Systems Division
Tel: 703-339-9550
Web: www.classifiedpc.com
Email: sales@classifiedpc.com