Oops! I lost my laptop

Don’t worry. It's not your fault. Is it?
After all, surely your IT Manager is the expert and should have put something on the machine to protect the confidential stuff. That’s right, he’s the expert; you’re just the humble user. How are you going to explain that extremely confidential company information, or government secrets, have risked being compromised because you were “tired and emotional”, and left your laptop in the back of a taxi?

Any IT Manager worth his salt should realise that with hundreds, if not thousands, of laptops out there, something like this was bound to happen. QED, it’s not your fault. It’s the IT manager who’s to blame. He didn’t do his job properly. It’s not you who should be sacked, it’s the IT manager. If anything, you should be thanked for having discovered this security loophole. In your dreams. Instead, you’re for the chop. Unless…

The Promise

Buy Black Whole, install it on your laptop and you can get as “emotional” as you like, and not worry about losing your laptop.
It doesn’t matter anymore. Even if it’s found by a tabloid journalist. Your secrets are safe with Black Whole, because it ensures that private data remains private, and is not compromised.

More about that threat, please

The risk that sensitive, confidential and private data may be accessed by an unauthorised person is greatly increased for the mobile user. Laptops, by their very nature, are lightweight and portable. So, they can very easily be lost or stolen.

So, what’s the panic? The straight cost of a lost laptop is easily covered; just insure it. What about all that lovely data you have lost? Well that’s easily covered too; back it up! OK, OK, so you don’t do back-ups. Well, the world is divided into two halves; those people who have lost data and now do back-ups, and those people who have still to lose data.

The real threat is the cost of your private data falling into the wrong (enemy) hands. And we’re not talking about the cost to your mental health at the thought of explaining the loss to your boss, or the IT manager, or the MD…

This threat could compromise financial details, lose your company its competitive edge, or threaten national security. But what can you do about it? The answer is simple; install Black Whole and we will make a more serious, and bigger promise.
The Serious Promise
Buy Black Whole, install it on your laptops and desktops and, as long as you take care of the first two threats yourself, (insure your equipment, and do back-ups!), we promise you peace of mind.

IT Security products have a reputation for being complex to implement, hard to use and, well, they just get in the way. Not Black Whole. With Black Whole you have security that doesn’t get in the way. How?

Pretty “fly” for an IT Security product
Black Whole is an on-the-fly disc encryptor. You take your folders with sensitive data, and encrypt them. Or rather, Black Whole does. When you open a file, it is decrypted automatically. The only time sensitive data is not encrypted is when it is being used; i.e. held in memory. Whenever it is held on disk, even in the swap file, it is automatically encrypted. So once installed and set up, Black Whole is transparent.

A list of authorised users for the PC is set up, and when authorised users log in, they just use their machine as normal. That’s the ‘Security that doesn’t get in the way’ part. When an unauthorised user tries to access the data, then the security definitely does get in the way. Even if someone steals your machine, takes it to pieces and puts the hard drive into a slave machine, they still won’t be able to get at your data.

How does it do it?
So if the normal user doesn’t have to do anything special, how is Black Whole operated and set up? Through a simple Control Panel applet that allows the PC administrator to set up users and instruct Black Whole how to behave. This allows separate security roles to be set up, so that different levels of control can be given to users of different levels of ability, need and trust.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal Users</td>
<td>Simply use the system as it is set up, and cannot change the set up. Data is automatically encrypted. Normal users can see which data is encrypted, but cannot set or change which data is to be encrypted.</td>
</tr>
<tr>
<td>Limited Users</td>
<td>Can also use the system as it is set up, but cannot decrypt any encrypted data or use any encrypted applications. This is ideal if you want a Service Engineer to have access to your machine but not to be able to see your private data or run specific applications.</td>
</tr>
<tr>
<td>Encryption Managers</td>
<td>The lowest level administrators. They can decide which folders are to be encrypted.</td>
</tr>
<tr>
<td>Decryption Managers</td>
<td>Middle level administrators. They can also decide to decrypt an encrypted folder.</td>
</tr>
<tr>
<td>System Managers</td>
<td>Top level administrators. They can define exceptions to the encrypt rules, set the login parameters, and set-up and manage other users.</td>
</tr>
</tbody>
</table>
Making life easy for the users

Black Whole is easy to use – it’s even easy to set up. Our development philosophy is that users come first – how can we make life easier for users. The result is a system totally integrated into Windows. Defining which folders are to be encrypted and which are not, is an extra menu item within Explorer or My Computer. System administration is through a standard Control Panel Applet. Even the login screen can be set to look exactly like the standard Windows login screen, except that it cannot be bypassed. Because it is transparent to users and easy to use means that user training is unnecessary. Even training of administrators is minimal, as operation is very intuitive.

Inside the event horizon – the technical bit

Encryption. Black Whole uses industry-standard encryption algorithms such as Triple DES. The encryption algorithm in use can be changed easily, by selecting from an ever-increasing list of algorithms. No encryption keys are held on the machine in plain format. All keys are themselves held in encrypted form. So accessing the disk with a disk sector editor will not allow your data to be seen. Encryption of data is selective, in that only sensitive data need be encrypted, which means that there is minimum impact on machine performance.

Secure login. Access to the machine itself is controlled through a secure login. This authenticates the user as a legitimate user of the machine (there may be several users on each PC). Only people entitled to use the machine can use the machine. Access to the machine is controlled by the entry of a valid username and a secret password.

Password recovery. But what if the legitimate user forgets their password? Are they locked out forever? What if they are out of the office; can the user be supported remotely so they can use their machine again? Well, in the spirit of ‘the user comes first’ Black Whole provides secure recovery facilities for just such an eventuality.

The recovery facility employs a full challenge – response system that allows the user who has forgotten their password to use a single, one-off, unique access code which allows them to logon to their account once, and once only. This recovery mechanism is secure and can be operated remotely over the telephone. Once a user has been recovered remotely, their password is set to a default to allow future logins.

For full technical details see the Black Whole Technical Overview.

What can I use Black Whole on?

Laptops, Desktops, floppy disks, zip disks…

By now, you can see that Black Whole is ideal for laptops, but what about desktops? Black Whole was specifically designed to meet the needs of laptop users, however, it is also applicable to the desktop environment. Even desktop machines get stolen, or
are left unattended and can be compromised. This is particularly true when using removable hard drives, which in themselves, can easily be lost or stolen.

Although desktop machines are not as mobile as laptops and are, therefore, not as easily lost or stolen, the floppy drives they use are mobile, and can easily be lost or stolen. Black Whole protects against this as it allows data on removable media to be encrypted. So even if a floppy disk containing sensitive data is lost or stolen, you are protected. The data held on it cannot be read by an unauthorised person.

Even your desktop machine is not attended 24 hours a day. So how do you know someone has not been tampering with your machine while you were away? With normal Windows, you don’t. But with Black Whole installed you do. It provides a login history, which gives the details of the previous last successful login and also the last failed login. The user is notified of the last login information at each login. So if someone has used your machine, you know about it.

**Data Protection Act**

The new legal requirements imposed by the EU directive, and subsequent changes in the Data Protection Act, mean that people responsible for systems which store personal details have a legal responsibility to take positive steps to stop this data from being compromised. So the law now says that private data about people must remain private. Installing Black Whole and encrypting all personal data complies with this. So not only does Black Whole keep you safe, it also keeps you legal.

**Is it for me?**

If you value the privacy of your data, and you want an easy-to-use, yet effective solution, then yes, Black Whole is of use to you whether you are a laptop user, a desktop user or both.