



Information Sheet

Using Otium Disk Space Reporter to deal with the risk of storing illegal and offensive data

In today's information age there is an inevitability that illegal or offensive data is being stored on your company servers. This is not something that we can turn a blind eye to. There are many instances of successful lawsuits against companies for holding MP3 music files and also distributing pornographic material. This is an issue that needs to be taken seriously.

Otium Utilistor Disk Space Reporter (DSR) enables companies to proactively investigate and manage the data that they are storing on their corporate network. When used as part of a clearly articulated electronic data monitoring policy, DSR can help ensure that companies do not lay themselves open to legal charges and upsetting employees.

If methods for investigating data are not put in place employees will store copyrighted data and offensive material such as pornographic pictures on company resources. Distributing MP3s is common-place and illegal. The bodies responsible for protecting music copyright are now proactively pursuing this offence in the corporate world. Pornographic data is also rife on company networks, if discovered or sent to people that find the images offensive, your company can be found liable.

DSR allows you to investigate data on your corporate network. It produces predefined reports that enable you to identify potentially offensive or illegal material.

DSR will find all multimedia files including mp3, WAV, GIF, JPEG, MPEG etc. It will allow IT staff to identify what servers, volumes, departments or staff that potentially offensive data belongs to.

Our advice is to use DSR in conjunction with a fair and clearly articulated monitoring policy. DSR provides the tools for IT departments to have a productive communicative dialogue with staff. DSR can be used in a non-prescriptive manner. If a legitimate reason exists for holding a particular type of file, that can be agreed upon. But likewise if data is being stored that puts your company in a vulnerable position, DSR will help you find and eliminate it.

Silicon.com report highlighted an outsourced help desk department where employees had set up a sub-network, unknown to the company, and was running an **escort agency and pirate software distribution**.

Headline from internetnews.com stated "Child pornography is hidden on virtually every large corporate network, according to security experts" Charles Kolodgy of IDC is quoted in the same article. He claims that it is not unusual for outsiders to "hack" into corporate networks and use available disk space to store this illegal data.

MP3 files can cost money. A consulting firm (Integrated Information Systems inc) received a **\$1million** penalty for running a dedicated MP3 server on it's network.

Employers have a legal obligation to prevent harassment in the work place. If employees inadvertently come across offensive data on the company network, this in itself can give rise to harassment claims. More serious still, is if this data finds it way to non-employees of the company.