



Lost Tapes?

A whitepaper from DISUK Limited

By Paul Howard

Lost Tapes?

Executive Summary

Every time there is a report of a loss of a backup tape, the standard response give out with the press release seems to go along the lines of “because our system is proprietary you could not read the tapes without a similar system”. This may make the person, trying to minimise the damage that having to publicly admit to the negligence that has allowed confidential customer data to be compromised feel better, but what is the reality?

For years certain system users were convinced that their information was secured by the obscurity of the system and maybe this is what encourages this attitude from the people generating the press releases. The supposition that anyone finding the tapes needs the same systems, and of course still needs to overcome the passwords that protect access to files, allows many a CIO to sleep soundly at night, but the reality is far from this.

If you have a backup tape from someone’s system XYZ , and you restore it on your system XYZ, you are of course the administrator on your system and can give user rights and access data restored to it. This means you can access all that data quiet easily, unless there are some very specific extra precautions being taken on the original system.

For years the IBM AS/400 community lived with the view that their system was a secure and safe system and looked out at all the security issues reported on the Windows servers with little disguised distain. They failed to understand even their backup tapes, written in EBCDIC (Expanded Binary Coded Decimal Interchange Code) can be easily displayed on a simple PC with a straightforward tape dump routine. It is quite straightforward to dump these details and start to use the information gained on that same simple PC. Identity theft using this method can result in millions of people being affected just by the loss of one tape.

Lost Tapes?

Another reason given in the past was that the thief or person finding a tape would not have the right tape technology to be able to read the tape as this was restricted to mainframe and midrange systems only. This is no longer true with very high capacity drives being made available at a low cost on the likes of e-bay and similar auction sites. Major companies see their large tape silos as very high price tag items but overlook that the drives contained in them are very often available to the world as low cost desk top devices. These units are easy to acquire at a low cost and may not transfer the data at the high transfer rates as those found in the large tape silos, but the tape formats are the same and then can be read easily.

We also often here the statement, we have no reason to believe the missing data has been used! The idea that this data must be used straight away to be of any use also shows a lack of understanding as to how this type of information gets used. The thief only needs to store the data and wait for the users to start to relax, maybe for the banks and credit card companies to minimise the monitoring of those accounts, and then they start to use the information gathered. SSN's, the users address, date of birth, place of birth and other useful information is not likely to change over and 18 month period so the thieves can afford to wait before making use of that data.

Sometimes we hear that everything is OK as the missing tapes have been found but this can be an even more worrying state. Where were the tapes, who had access to them and could they have been copied whilst they were missing? In this case the compromised account may not be flagged up for special monitoring of unusual activity so can be more at risk than those tapes that are deemed missing.

A worrying trend that is becoming apparent is the increasing number of tapes that are being flagged as having been stolen. This might simply because the reporting process has been improved but may indicate that as security on the electronic access to systems has improved so thieves have started looking at simpler ways to get the information they trade. High capacity tapes now can easily contain over one million complex records so their value grows to the thief.

Lost Tapes

Some people may be considering that if these tapes contain such valuable information, why are they being transported around and getting lost and stolen all the time. Tape backup is still the most common way for companies to ensure that in the event of some catastrophe they are easily able to get their business back up and running. Tapes that are not taken off site to somewhere unlikely to be affected by the same catastrophe as the main site are useless, so all professional IT staff ensures they get a daily backup removed to a place of safety.

Another worrying comment is that “there is no indication that the data has been compromised” as trotted out by the UK Government after they admitted the loss of 25 million records on removable media. There seems to be a misunderstanding that any stolen records will be used immediately but again this is not the case. The basic information will still be valid after more than 12 months have gone past in most cases and can still be used long after that so just because they are not used within the first four weeks of a loss does not mean they are in the hands of people who will use them fraudulently.

Encryption is simple, available to all systems and drive types and needs passed no software, drivers, or agents to be added to the system so why aren't all companies that hold private and confidential data encrypting their backup tapes.

DISUK Limited
Silverstone Innovation Centre
Silverstone
Northamptonshire
NN12 8GX
United Kingdom

Tel: +44 (0) 1327 856070
Fax: +44 (0) 1327 856071

Web: www.disuk.com
Email: Sales@disuk.com



Copyright © 2006 DISUK Ltd. All rights reserved.

The trademarks, logos and service marks (“Marks”) displayed herein are the property of DISUK or other third parties. You are not permitted to use these Marks without the prior written consent of DISUK or such appropriate third party.

All other trademarks mentioned in this document are the property of their respective owners.