PROBLEM REF PC0066318
Incomplete TMS Audit Trail
Problem Manager - Graham Hooper
Date Raised 24/05/2001

Customer reference 1000520

Diary

24/05/2001 14:21:21 - By Graham Hooper
CALL PC PC0066318
Incomplete TMS Audit Trail

Problem origination - CS Security in undertaking audit file data extractions. Notification to PON Internal Crime Manager (Charles Leighton) on 9.5.01 advising that we are unable to source evidential data.

Details of problem - An incomplete TMS audit trail for the period 8th to 14th August 2000 caused by coincidental DLT failure at both datacentres. This was compounded by a loss by TNT Couriers of one tape in transit to FEL01 for analysis. All other elements of the audit trail are complete. Pathway is in contractual non-compliance until 15.02.02 (there is a requirement to retain audit data for 18 months). Pathway cannot meet Requirement 699 and 829 in respect of these dates.

Temporary procedures - none

Current action - ICL Pathway have attempted to recover data from the Bootle tape both internally and external via data recovery experts. The latter has concluded that there is a flaw in the DLT media and recovery would only be 85% successful. This is no more than we could do ourselves. A similar scenario would have been expected from the lost Wigan tape. A letter was sent from Jan Homes (Pathway Audit Manager) on 23.5.01 to Sue Kinghorn (Consignia Internal Audit) to advise of the problem

Next steps - Notifying the PON Problem Manager (Richard Benton GRO and advise. We are writing to TNT Couriers to request and ongoing search for the mislaid package although in the event of locating the missing package our chances of restoration of all data is highly unlikely. Update problem database.

Next update - following discussion with Richard Benton on 23 May, 2001.

Closure Criteria - tba

POCL Reference -P1000520

The Problem Manager Assigned for ICL Pathway is Graham Hooper/Jan Holmes.

29/05/2001 17:28:38 - By Janet Reynolds
Update received from Graham Hooper:
23/05/01 19:17:20 - by Graham Hooper

Advised by Colin Lenton-Smith that at the CAB today Keith Baines raised the issue over the 6 days data loss. He said he would discuss the significance of this with Charles [Leighton]. He raised two additional questions:

1. What is the security impact of the lost tape - could a third party identify what the data is?
2. What are our processes for validating data held?

A response will be provided by cop 24/05/01.

24/05/01 10:15:57 - by Graham Hooper
I spoke with Richard Benton and outlined the issue. I stressed that back-ups were taken and the problem resulted from a corruption of both tapes relevant to the period in question - a situation that could not reasonably have been foreseen. It is clear that Consignia's prime issue is in attempting to recover the lost data - primarily in respect of evidence to support potential prosecutions. I advised that both Pathway and Vogon Data Recovery had undertaken an analysis of the Bootle tape and concluded that not all the data could be recovered. The cause of the read error on the Wigan tape is unknown and resulted in the decision to forward this to FEL01 for analysis (during which it was lost by TNT). Richard asked why the Wigan tape was not copied prior to dispatch to provide a backup. I advised that this was not possible as the tape would not read and therefore could not be copied. This was accepted. It was agreed that the only reasonable progression was to try and locate the lost Wigan tape so that an analysis and data recovery attempt could be performed. To this end I advised that I had been trying to get TNT to undertake a search but was not content that TNT were doing all they could to find the tape. I was today writing a letter to the TNT Customer Accounts Manager to escalate the issue.

I also advised that Jan Holmes (Pathway Audit Manager) had written to his opposite number in Consignia (Alison Kinghorn) to advise of the issue. Richard asked for a copy of that letter which I will forward.

24/05/01 2:39:16 - by Graham Hooper
Response for Colin Lenton-Smith provided in conjunction with Jan Holmes:

1. What is the security impact of the lost tape - could a third party identify what the data is?

Answer:
The information written to Legato tapes can only be read by dedicated Legato scanning software and hardware or by specialist data recovery equipment. In the event that a third party obtained the necessary Legato equipment and software, it is evident from the fact that the tape could not be read on the dedicated equipment at the datacentres that any attempt by a third party to do the same would not prove fruitful. Specialist data recovery equipment is available primarily to forensic recovery experts such as Vogon International, to whom Pathway referred the corrupted Bootle tape for analysis. These companies operate strict controls to ensure that data recovery is attempted only for legitimate reasons. Assuming a third party succeeded where ICL Pathway failed or managed to utilise other specialist recovery services, the information on the tape is not in a readily interpretable format and it is not possible to infer to what it relates. NINOs, DSS Order Book numbers, dates, amounts and Outlet codes would be evident but a third party could not determine solely from this either from where the information originated or to whom it related. In addition, the tape in question does not contain any label or other identifying marks that would indicate its contents or source.

2. What are our processes for validating data held?

Answer:
The validity of the data held, and subsequently retrieved, is proven through the generation of a ChecksumSeal at the time that the data is written to the DLT. This value is stored on a database, separate from the audit data, and subject to an entirely independent backup process. When data is retrieved from the DLT the Checksum Value is re-calculated and the result compared with the original value maintained in the database. The results are recorded in the database and these are checked as part of the Extraction process prior to despatch of data to PON.
It is possible to conduct a read-after-write activity on the DLT after each session. This has been considered in the past and is the subject of ongoing debate. We have taken the view that this would not be necessary for the following reasons :

FUJ00152184

a. Audit data is written to two separate DLTs, one at each Data Centre, thus providing a second copy for backup and resilience.
b. The data is appended to DLTs over a period of weeks thus the tape is subject to repeated read/write activity during the normal operation.
c. There is a time penalty in conducting read-after-write which would have an impact on already tight schedules for the Legato drives.
There are a number of specifics which should also be taken into account : · The two DLTs originated from two different batches. · We did not experience a write failure during the creation of this DLT over the period in question. This is evidenced by Save Set status available from the Legato system

24/05/01 3:40:12 - by Graham Hooper
Richard Benton advised of Pathway call reference.

29/05/01 11:02:27 - by Graham Hooper
Letter drafted by GH and sent to TNT Couriers by Jane Hassard on 25/05/01 requesting assistance with chasing the location of the missing package.

Paul Westfield queried status of problem. Advised that Database entry has been made, PON Problem Manager has been engaged and d/b updates being provided.

03/06/01 10:30:00 - by Graham Hooper

Response received from TNT Couriers apologising for the loss and stating that there had been a discrepancy in the tracking system, which could have contributed to the problem. They fear that the original addressing may now be incorrect.
I am convinced that they are not trying hard enough to locate this package which must be somewhere in their system. I propose to respond and to ask that a search of all unaccounted-for items be made.

12/06/01 10:55:37 - by Graham Hooper

In order to provide some assurances that other Legato tapes are not corrupted, Pathway/ISD propose to introduce write failure checking on archive tapes. Dates for introduction are being clarified.

26/06/2001 08:55:59 - By Jean Woolley
19/06/01 11.05.28 - by Graham Hooper

Joint Security Audit meeting held attended by Jan Holmes (ICLP Audit Manager), Gary Potts (PON Audit), Charles Leighton (PON Internal Crime Manager) and Graham Hooper. The issue of the missing audit data was an Agenda item. Both Jan Holmes and I explained the issue and answered questions about the circumstances leading to the problem, which were difficult to anticipate.
Sourcing the missing data from elsewhere is unlikely although ICL Pathway will do what it can. The important thing was to ensure that we take action as far as possible, to obviate a re-occurrence. We advised that ICL Pathway would be introducing a "read after write" procedure that will provide assurance that data is not corrupt when written to tape. PON requested that the next joint Audit of the datacentres include tape-handling procedures. ICL Pathway is content with this and will undertake with PON in September. TNT is no longer being used for the transport of media or other sensitive audit/security information.

20/06/01 15:21:10 - by Graham Hooper

Second letter sent to TNT from Graham Hooper stressing the importance of finding the missing item and offering assistance in attending TNT sites to identify the package. Awaiting response.

25/06/01 15:43:01 - by Graham Hooper

The introduction of the "read after write" procedure has been approved for S06 release and is currently being tested.

26/07/2001 11:27:30 - By Jean Woolley
11/07/01 17:37:12 - by Graham Hooper

No response received from TNT in respect of letter sent on 20/06/01. Chase up letter issued.

01/08/2001 14:20:44 - By Jean Woolley
30/07/01 08:18:09 - by Graham Hooper

Confirmation from Pathway Development that SO6 testing on read after write has been completed. Automated Media Management (to automate tape labelling) will be introduced on 20/8/2001. Cloning for read after write will be switched on 3/9/2001. Awaiting response from TNT to second letter.

14/08/2001 10:01:29 - By Jean Woolley
13/08/01 08:04:39 - by Graham Hooper

Routine housekeeping at the Datacentres has established the existence of a number of backup tapes, which may span the lost data period. An internal change request has been raised to establish the periodicity of the tapes and whether they can be used to reconstruct the missing audit trail.

Response received from TNT stating that they have recently introduced a database of missing items, which can be searched against details of package contents. Details of the lost tape confirmed. They will attempt to establish whether the tape and/or package is recorded on the system.

24/08/2001 12:55:32 - By Jean Woolley
23/08/01 14:54:50 - By Graham Hooper

Formal response received from TNT. They have carried out an extensive check of their TNT I.D Stores database against the description parameters supplied for the lost tape. None of the items listed as possible candidates provides a match for the DLT. TNT conclude that they have undertaken everything possible to locate the lost tape and apologies for the difficulties this has caused ICL Pathway and any other third party. I am now satisfied that there is no possibility of finding this tape. In any event it needs to be borne in mind that the tape in question was corrupt before despatch so the likelihood of data recovery from it was negligible.

The CP raised to explore the possibility of recovering missing data was approved by CCB. Work will now begin on building the appropriate platforms as a precursor to undertaking recovery.

04/10/2001 14:52:10 - By Jean Woolley
Update by Graham Hooper
01/10/01 15:40:31 - By Graham Hooper

Backup tapes recovered from datacentre and held in secure fire-safe storage pending attempted recovery. Recovery plan being finalised by Audit Development. PTI awaiting purchase and delivery of disks to build pseudo Audit Server.

12/10/2001 15:47:59 - By Linda Gaskin
Updated - By Graham Hooper

Required disks delivered and recovery plan has been finalised. Pseudo Audit server will be built during w/c 15/10/01 with a view to beginning recovery activities on 22/10/01.

22/10/2001 10:13:57 - By Jean Woolley
18/10/01 06:45:38 - By Graham Hooper

Build of Audit Server underway. CP re-impacted and re-targeted as additional configuration delivery identified for live.

13/11/2001 13:25:28 - By Jean Woolley
Update by Graham Hooper
The build of pseudo Audit Server and peripherals has been completed. Work has begun on loading backup tapes but problems have been encountered with the PIT rig Autochanger, which is reporting a device failure. An engineer is currently looking at the problem. It is anticipated that necessary repairs will be completed today and recovery work can continue.

14/11/2001 09:08:28 - By Jean Woolley
14/11/01 08:24:13 - By Graham Hooper

The PIT rig Autochanger has been repaired. Recovery work is continuing.

04/12/2001 10:26:33 - By Jean Woolley
03/12/01 11:38:51 - By Graham Hooper

Work is nearing completion on loading all backup tapes onto the pseudo PIT Audit Server rig as a precursor to reconstituting the audit archive. The periodicity of data contained on the tapes is emerging. It appears that whilst most of the missing audit trail can be recovered we may be left with a period of 2 days for which we will be unable to reconstruct the archive. We should have a complete picture by the end of the week and a full update will be provided then.
10/12/2001 12:03:54 - By Graham Hooper

Work has been completed on the loading of all backup tapes onto the pseudo Audit Server rig and undertaking a full scan of the contents. We have now been able to determine the extent of the data they contain and our ability to recover the data.

It is now clear that we are able to recover some 66% of the missing TMS data between the 7/8/2000 and 14/8/2000. The other 34% is not present on the tapes and is irretrievable. The recoverable data is present in a number of partitions across the 4 Correspondence Servers for the period in question. In respect of RFI 8 (the request that highlighted the existence of the break) the unrecoverable period is from 19.27 on Sunday 6/8/2000 until 16.09 on Monday 7/8/2000. This compares to the original reported break of 8/8/2000 to 14/8/2000 (late hoarding caused late reporting of the problem).

We intend to brief Consignia Security and Audit Managers with a view to determining how the issue should now be progressed.

07/01/02 11:18:31 - by Graham Hooper

Consignia Internal Audit and Security Managers have been briefed on the outcome of the data scanning activities. In respect of RFI 8 (the request that highlighted the existence of the break) the unrecoverable period is actually from 19:27 on Sunday 6 August until 16:09 on Monday 7 August. This compares to the original reported break of 8 August to 14 August inclusive (late hoarding caused late reporting of the problem).

Consignia Security has confirmed that the information requested on RFI 8 is not at this stage required in support of a prosecution although this may change. It has therefore been agreed that ICL Pathway will not need to recover this lost/found data at the moment, but will take steps to ensure that the information on RFI 8 is stored and made available for recovery if requested to do so at a later date.

The cause of the lost data was a coincidental tape failure at both Datacentres. Analysis of the Bootle tape confirmed the presence of a flaw in the DLT media, which would have accounted for the inability to read the contents. We can currently only speculate on the cause of the read error on the Wigan tape since it was irretrievably lost by TNT Couriers during transit to FEL01 for analysis. ICLP are presently undertaking out a root causal analysis of DLTs to see if there is any common characteristic(s) that would indicate the likely reason.

ICL Pathway has also introduced a number of additional measures to help avoid a recurrence:

- a "read after write" procedure to provide assurance that data is not corrupt when written to tape and to protect against the accidental use of flawed media;
- · Automated Media Management to automate tape labelling and thus reduce manual intervention;
- · TNT Couriers are no longer used to transport audit or other sensitive media.

In addition, tape-handling procedures were reviewed in conjunction with Consignia Internal Audit as part of the Joint Audit of the datacentres and the possibility of full tape cloning is being investigated to provide a greater degree of resilience.

Whilst the action outlined above mitigates a recurrence, ICL Pathway has advised the Head of Horizon Commercial and Consignia Internal Audit and Security Managers that measures to remove altogether the risk of future tape corruption can be achieved only by a complete re-design of the current solution.