Appendix L: Issues arising from the failure of the library management system

Cause of the problem

1. On the 3rd March, the Vubis library management system failed, and has been unavailable since. Emergency backup systems are in place for critical library functions (issue & return of books) and use of self-service kiosks. Wifi services and access to public PCs, printers and other equipment have since been restored.

2. The incident occurred due to a combination of server and system errors. On 2nd March, Infor (the third party support provider for the Vubis application), reported to LBB Libraries that the library system was running out of space on the server. Customer Support Group (CSG) responded to provide additional physical storage. At this time, it was unknown that back-ups for the system had been failing since the end of December 2015 (unrelated to the storage issue). The automated messages from Vubis alerting a nominated user of back-up failures were not being received. Investigations to understand why these were not received are hampered due to the corrupted database. Consequently, the back-up failed again, causing the system to crash and corrupt.

3. When the server was rebooted, it began to corrupt the data on the system. Whilst local backup processes were put in place these were backups to the local machine which also corrupted. The root cause analysis (RCA) has been concluded to be as follows:

4. A number of disk drives on the server displayed hardware failures. These were replaced and the system was left overnight to rebuild. This is a standard system administrative function to resolve a failed disk. Subsequently the server crashed around 03.54 on 3 March and it is believed that the database files on Vubis became corrupted as a result of, or during, the subsequent required reboots.

5. A local backup process was put in place where data was backed up daily to the Vubis server as part of the system functionality. According to an investigation from the application support provider (Infor) these local back-ups had started failing from 26 December 2015. System alerts were not received reporting this failure. Investigations to understand why these were not received are hampered due to the corrupted database.

6. The pilot technology enabled opening (TEO) at Edgware library is unavailable as the entry system user verification feature requires a check between the card, the PIN and the Vubis database.

7. A non-corrupted tape back-up from March 2014 is available – this is the last date a tape back-up was carried out as the server was changed to digital back-ups only following this date.

8. Work is underway with the 3rd party support provider, Infor, to recover data from the corrupted system with the target date for completion by 31st March 2016. The agreed approach is to add this recovered data to the restored 2014 back-up and supplement with data held from adjoining systems and manual records where available.

9. The Vubis system consists of different data types such as book, barcode, borrower and transaction data which are in various conditions for recovery. However, borrower data is recoverable, as is some of book information.

The effects of the problem

10. Customers can borrow and return books in libraries. Wifi in libraries has been restored. However, renewals are not currently possible due to inadequate transaction data in the system, and fines are currently being waived. The current library catalogue is unavailable. PC access for Adults is available, but not for children as there is no way of validating parental consent via an online tool. Manual workarounds continue to be investigated and implemented.

11. The extended opening hours at Edgware library are suspended as the entry system requires a check with the Vubis database (see above).

How it will be resolved

12. We have recovered all of the information that is possible to recover from the system that is not corrupted. Infor and the CSG teams are working together to make the system available again by the target date of 31st March 2016. A workaround has been created with the TEO supplier to break the link with the library system while the latter is repaired. Available IT services inside the TEO library will match that of staffed libraries during the unavailability of Vubis. This means that the library catalogue, renewal of books, reservations, some e-books and e-audio books, and access to PCs for children and teenagers (due to parental consent being stored within Vubis) are unavailable at present. Manual workarounds continue to be investigated and implemented and notified to users as they become available.

13. Once the Library Management System (Vubis) is restored, it is estimated that it will take the libraries service 3-6 months to fully populate the gaps in the data. In the meantime, libraries will be open and services will be restored as the data gaps are populated. The extended opening hours at Edgware will be able to be available during this process (see below).

14. TEO requires names and PIN numbers to be able to operate. Verification between the door entry panel and the library management system is not available as the latter has failed. Entry into the building using TEO is therefore not currently possible.

15. Names have been recovered but PIN information is irrecoverable. PINs will need to be reissued. A step by step process to re-establishing the service, based on the time required to communicate to all registered users of the TEO service, has been created. Registered TEO users will be notified of the new PIN by the 1st April, ready for the target date for re-opening of the TEO hours of the 1st April.

How it could be prevented from happening again

16. Since 6th March, new infrastructure has been built with increased physical resilience in place to back up the system to a secure offsite backup service. A similar issue could arise only if the server, software and secure back up service were all compromised. While not impossible, this would be an extremely unlikely scenario. An extra layer of protection has been added in now having off-site back-ups. This means that the impact of any future outage would be downtime of hours rather than weeks.

Contingency measures in the event of a similar incident/complete outage of database/technology

17. In the event of a future whole system data failure, a core library service at Core and Core Plus libraries would be maintained through the deployment of additional staff at an estimated cost of £75k per month. This would be a mix of temporary agency staff and security staff with extra hours and overtime for permanent staff. It is assumed that it would take 1-3 weeks to secure the services of, and train, additional staff.

18. If the system were to fail again while customers were in a core library service at Core and Core Plus libraries, this would not affect a customer's ability to leave the building. TEO works on entry only – to exit there is a door push button that is independent of the TEO system which would still operate. There are also push-bar emergency exists and if the alarms are activated or there is a power failure the doors default to open.

19. The core library service would operate from 9 to 5 over six days at Core Plus libraries and five days at Core libraries. The contingency plan would be implemented in line with the following timetable:

    - Week 1: maintain advertised staffed and volunteer opening hours in Core Plus and Core libraries
    - Week 2 : offer 9-5 opening in Core Plus libraries (and maintain advertised staffed and volunteer opening hours in Core libraries) through the deployment of security guard/agency staff for hours outside of staffed/volunteer hours

- Week 3: offer 9-5 opening in Core Plus and Core libraries through the deployment of security guard/agency staff for hours outside of staffed/volunteer hours