POL00142856

Post Office Ltd – Strictly Confidential

POL()

POST OFFICE LTD – POL BOARD NOTING PAPER

Horizon

1. Purpose

The purpose of this paper is to:

1.1. Brief the board on the Horizon service.
1.2. Update the board on the recent major incidents on Horizon.
1.3. Outline the actions being taken to prevent further failures.

2. Background

2.1. Last week's major incident on Horizon was the fourth significant service failure of this system in nine months. Briefly summarised, they are:
- 27th July 2011 – Pin pad failure caused by a change activity
- 12th December 2011 – Horizon service failure caused by a hardware failure
- 1st February 2012 – Card account failure caused by a change activity
- 1st March 2012 – Horizon service failure caused by a hardware failure

2.2. When the Horizon service was initially constructed it was based across two data centres, both of which were fully operational; providing an active/active resilient service arrangement.
2.3. As part of the move to Horizon on Line, the contract was renegotiated and the architectural design changed in order to reduce Post Office's operating costs by £50m p.a. (excluding VAT). One of the design changes which contributed significantly (circa £5.5m p.a.) to the savings was moving to an active/passive data centre arrangement. Consequently the resilience is now housed in one data centre with the second data centre primarily being used as a test environment, but available for disaster recovery if required.
2.4. As a consequence of moving to the active /passive design, when hardware issues arise they will result in network wide service disruption.
2.5. The previous active/active data centre arrangement would have prevented an impact to customers for the incidents of the 12th December and the 1st March, as the hardware would still have been working in the other data centre.

3. Current Situation – Incidents

3.1. The incident on the 1st March was caused by a network router within the data centre restricting the flow of transactions to the data centre. As it was in effect still working, the device advertised itself as available and no alert was raised.
3.2. The router started failing just after 11am and from that point on branches would have seen transactions going through the system much slower than normal. Many transactions were going through so slowly that they timed out. From around 11:10 we were seeing less than a fifth of the expected volume going through the system; and the situation continued to deteriorate.
3.3. By 14:15 Fujitsu had identified the component causing the issue and asked for Post Office approval to replace the device. Replacing the router would cause a few minutes outage of the service. As the service was in a critical state, swift approval was given and the service was restored at 14:25.

POL00142856

3.4. In terms of the two hardware failures, these related to different components within the Horizon data centre. Whilst backup devices were available in both cases they didn't activate due to the way in which the failing hardware acted.
3.5. With regards to the two incidents that were caused by change activities. Both of these relate to updating our product reference data on Horizon. July's incident was due to the correct processes not being followed. Whereas February's incident was due to the test processes for reference data changes and changes delivered through a programmed release not being fully cognisant of each other.
3.6. All of the above incidents are subject to ongoing operational investigations. A number of changes have already been made to both the reference data processes and to the hardware. See section 6 for further details about the proposal for a strategic review to complement the actions that are already underway to prevent recurrence.

4. Service Levels

4.1. The availability service level is measured across the network of counter positions where they are able to perform all transactions. The Counter Availability metric is defined as the number of counter position hours available as a proportion of the maximum number of counter position hours available based upon the Post Office Core Day (08:00hrs – 18:00hrs Mon – Fri, 08:00-13:00 Sat).
4.2. Liquidated damages (£3.50 per unavailable counter hour) are payable if the unavailable counter hours per month exceed the equivalent of 2.37 hours per counter in the month.
4.3. If the cause of unavailability is a network wide failure event then the contract allows Fujitsu to cap the damages at £400k for that event.
4.4. This has resulted in the following in respect of the four incidents:
- July's incident – a settlement of £250k was agreed
- December's incident – no Liquidated Damages are due as the total unavailability in the month did not exceed 2.37 hours per counter
- February's incident – yet to be confirmed but looks unlikely that Liquidated Damages will be due as the availability in the rest of the month was good and overall unavailability in the month did not exceed 2.37 hours
- March's incident – the amount of Liquidated Damages due is dependent on the performance in rest of the month.

5. Risks & Mitigations

5.1. Since the move to Horizon on Line the disaster recovery service has undergone several tests, incrementally these provide a level of assurance. A full data centre failover is the only test which hasn't yet been proven and is an outstanding risk which we aim to address at the end of the month.
5.2. The data centre failover which provides the end to end test assurance means failing over from the active data centre to the passive data centre and is scheduled for the weekend of 31st March/1st April. This will be the first of its kind since the move to the active/passive data centre set up.
5.3. Credence is also hosted in the Fujitsu data centre. Last year Credence had no disaster recovery service and was involved in the process of delivering transaction files to clients. Therefore had we conducted the end to end disaster recovery test at that time it would have meant holding back client transaction flies for 3 days. This risk was deemed unacceptable.
5.4. Business cases have been approved and action taken to move the delivery of client files from the Credence environment. This service moved from February and enables the data centre failover test to take place without the risking the delivery of files to clients.

POL00142856

6. Proposal

6.1. We will continue to conduct the operational investigations into each incident and make the improvements required to ensure the short term stability of the service.

6.2. In recognition of the recent performance history, the media attention this has drawn and our business transformation plans, we have proposed a fundamental review of the service. Within this review we will draw out whether the current technical design is correct for our future business needs and plans. The review will run in conjunction with the operational investigations.

6.3. We are proposing that the review will be conducted by Fujitsu and Post Office Ltd with involvement from independent partners. The review will run under the governance of a steering board consisting of the Executives from both organisations.

6.4. The review will as a minimum cover:

- The technical design of Horizon
- All forms of testing
- Monitoring and alerting
- Best practice in retail and financial service markets
- Future requirements of our business strategy that may influence the technical environment of which Horizon is a critical part.

6.5. The POL Board and the POL Executive Team will be invited to visit the data centres and receive regular updates on the progress and findings of this review.

7. Recommendations

The POL Board is asked to:

7.1. Note the actions being taken to protect customers from further disruptions to these services.

Mike Young
Chief Operating Officer
March 2012