ICT Systems Disaster Recovery Review

September 2016

Dave Thexton: ICT Manager

Keith Harding: Service Helpdesk Manager

Julian Parsons: Head of Service Development

1. Introduction

Buckinghamshire and Milton Keynes Fire and Rescue Service (BMKFRS) is categorised as a category 1 responder within the Civil Contingencies Act 2004 and is therefore expected to have developed robust business continuity plans to enable it to fulfil its statutory responsibilities for emergency response at all times.

The typical characteristics of High Reliability Organisations include:

- Problem Anticipation;
- Containment of Unexpected Events;
- Root Cause Analysis of Incidents/Accidents.

Using these three principals the BMKFRS ICT department has recently carried out a review of the vulnerability of the existing hardware and software systems. The timing of this review has been triggered by three events:

- A scheduled review of Disaster Recovery of ICT Infrastructure as a result of a recent review of BMKFRS wider business continuity plans;
- A recent increase in the number of cyber-attacks globally including a recent concerted attack on BMKFRS infrastructure.
- A recent ICT Health Check penetration test carried out in preparation for connection to the new Emergency Services network (due to go live in September 2017)

The review consisted of research of current best practice for resilient ICT infrastructure and consultation with the ICT personnel and the Information Governance Officer (IGO).

2. Executive Summary

It has been identified that a key vulnerability for the Service is the fact that the disaster recovery server array is contained within the same server room as the main server array. This was initially intended as a temporary arrangement but due to changes in the estate strategy this is liable to still be the case for the next two years. This presents an unacceptable risk to the Service.

By moving our disaster recovery to the Cloud will eliminate this risk and improve resilience. It will also allow a ‘try before you buy’ scenario for potentially moving our infrastructure to a Cloud host in its entirety, for sound business reasons and compliance with current Government policy.

It has been identified that there are some vulnerabilities for the Service through the increasing threat of cyber-attacks. The increasing sophistication of these attacks and the evolution of polymorphic viruses has highlighted this.

Through a combination of investment in the latest cyber-attack prevention software, staff education as to identification of suspicious emails and improved recovery time through better data management, the Service can improve its resilience to such attacks.

3. Hardware Systems Disaster Recovery

During the critical analysis of BMKFRS ICT systems the following hardware vulnerabilities have been identified:

- Co-location of the main server array and disaster recovery array in the same room (server room at Service Headquarters (SHQ));
- Main Data Feed Interruption;
- Failure of Back-Up tapes;
- 'Updata' connections.

3.1 Server Co-location

It has been common practice to back up the business as usual server array with a duplicate set of disaster recovery servers in a geographically separate location configured to automatically switch over when the main array fails. Previously the DR servers were located in the old control centre. We obviously had to decommission this facility after TVFCS came online. Initially the BMKFRS back up servers have been located in the same server room as the main servers. This was intended as a temporary arrangement until a second facility could be provided at a geographically remote location. Initially this was intended to be at Broughton Fire Station but this plan was changed with the successful bid for transformation funding for the Blue Light Hub in Milton Keynes. Currently, it is looking like at least another two years until the station is finally constructed and a new backup server array can brought online. The current feeling in the ICT department is that this is an unacceptably long time to tolerate this risk.

The threat is that a fire, long-term power outage or air conditioning failure in the server room would cause both the main and back up servers to fail. Such a failure would be catastrophic to the service critical and routine operations. The current plan to recover from this disaster would be to buy new servers and use back up tapes to install the last saved data files. This would take weeks rather than days to achieve.

We currently have some mitigation for the above risk. The power supplies are protected through UPS / and then the station generator. The air conditioning systems are constantly monitored and has redundancy. One of the systems is protected though the stations standby generator.

However, any failure of these systems, a fire or loss of HQ (such as an event that happened to South Oxfordshire District Council) would cause total system failure.

There was a near miss earlier this year when the road works took out the main supply cables to HQ. The redundancy systems operated as anticipated but this put a tremendous strain on the remaining air conditioning unit to keep the servers cool. Had the power outage lasted a few more hours there was the risk of partial or total system failure.

Potential Solutions

Option 1. Create a new DR server facility at Broughton as originally planned. This is not likely to be feasible or desirable as it would mean alteration works at Broughton as some of the existing space/capacity has been leased to Thames Valley Police. This would mean potentially losing some of the revenue from TVP or the capital costs of developing a new facility. New servers and associated infrastructure would have to be purchased, as the current DR servers are due for replacement in 2017.

Option 2. Create a new DR server facility at the new site at Ashland. This is not likely to be online for another two years. This is currently deemed, by the ICT management, as an unacceptably high risk for BMKFRS. New servers and associated infrastructure would have to be purchased, as the current DR servers are due for replacement in 2017. Currently space for this facility has been identified on outline plans for the site but this floor area could be freed up for other use.

Option 3. Decommission the existing DR server and move our DR to the Cloud through a recognised third party provider that satisfies our DR recovery requirements and data protection needs.

Current government policy is to encourage public services to migrate services to the Cloud or remote hosting. BMKFRS has a current policy of migrating systems to remotely hosted solutions. The BASI project has been successful in achieving this with the new systems.

https://www.gov.uk/government/news/government-adopts-cloud-first-policy-for-public-sector-it

At the Audit and Overview meeting 2 December 2015 an updated revised ICT Strategy was presented and noted. Within the updated strategy the following mission statement was presented.

The KIS department will deliver integrated solutions on robust, resilient and secure platforms. Wherever prudent, solutions should be remotely hosted or cloud-based. The applications, where appropriate, should be accessible through a range of modern mobile technologies. KIS functions will be supported by a team of cross-skilled, well-trained, and continuously developing technicians with a strong customer focus. Where possible services will be delivered through collaboration.

Moving the DR Server to the cloud has a number of advantages:

- Completely eliminates the risk of collocated BAU and DR servers;
- Removes the need for imminent and future capital costs of replacing the DR servers;
- Reduces power costs and carbon footprint;
- Reduces the capital costs of adding extra servers to cope with the increasing data storage requirements;
- Fits in with current HMG policy;
- Transfers the costs of managing servers to a third party;
- Reduces the associated server licensing costs to us;
- Provides BMKFRS with the opportunity to experiment with Cloud hosting to enable a decision on whether we wish to go for complete migration of our ICT infrastructure.

Cost comparison of Option 3 and server replacement.

Using a cloud provider for our DR is categorised into three potential solutions.

- **Cold.** Our DR system is periodically updated with our data. When it is required due to a system failure the DR system is brought on line in a systematic and predetermined way which would lead to a gap in services in excess of 15 minutes.
- **Warm.** Some key systems will be replicated in real time while other periodically updated. This will reduce the time there will be a gap in services and the key services will be no different from the BAU systems.
- **Hot.** All key systems will be replicated in real time through a live link. In the event of system failure the transition to the DR system will be nearly instantaneous and appear virtually seamless to end users.

The costing for these options are as follows:

	Monthly cost	Implementation
Cold	£478.00	£22,260.00
Warm	£975.47	£27,030.00
Hot	£1344.26	£31,800.00

Our current disaster recovery servers have an estimated useful life of five years, although this tends to be stretched to about six years. The purchase cost of a new server is £120k. The cost of the 'hot' disaster recovery solution for six years is £88k (based on £32k [+ 25% contingency] one-off expenditure and then a net additional cost of £8k per annum [as the subscription is £16k p.a. but there are £8k worth of licensing savings]).

Over the first six year period, there is a net saving to the Authority of £32k. In future cycles the savings will be even higher (c£72k) as the one-off implementation cost is not re-incurred.

Recently the MOD has moved a significant part of its ICT operation to the new Microsoft data centres in the UK. Providing secure operating for both its BAU and DR systems.

http://www.governmenttechnology.co.uk/news/07092016/microsoft-announces-operation-uk-cloud-data-centres

Recommendation 1: That the DR servers are decommissioned and our DR functions are moved to a Cloud provider that satisfies our operating and data security needs. The most suitable option for BMKFRS is a Hot configuration. The budget for this is based on the costings indicated above plus a 25% contingency for unforeseen consultation or system configuration and data requirements. The implementation costs are provided through an in year virement from identified underspends in contingency.

3.2 Updata Connections.

Part of the ICT infrastructure for the service is provided through a company called Updata and in partnership with Buckinghamshire County Council (BCC). This company provides interconnectivity for the Service's different sites through a robust network. The resilience is achieved through Updata's two network centres. One is located in Aylesbury and the other in Amersham.

To date this arrangement appears resilient and satisfies our needs. The arrangement is periodically reviewed through our partnership with BCC.

Recommendation 2: Our network arrangements with BCC, provided through Updata, continue to be satisfactory and should continue for the remainder of the contracted period.

3.3 Main Data Feed Interruption

Currently we have a vulnerability in that our network and data is supplied through to SHQ in a subterranean cable. It is a single cable and, like our power supply, is at the mercy of failure through a third party interrupting the supply (i.e. road works in the vicinity).

By moving the Services DR system to the Cloud would mean that our systems can be configured and our ICT systems can be operated independently from other FRS locations through the internet. This will provide greater resilience to the Service and eliminate this single point of failure.

Recommendation 3: By moving to a Cloud based DR arrangement our single point of failure in having a single data feed into SHQ will be eliminated.

3.4 Back-Up Tape Failure

Part of our recovery plan for loss of data due to system failure is that regular tape backups are made and then stored in a geographically remote location until needed.

After a recent system problem and subsequent data loss the backup files were discovered to have an unforeseen corruption which meant an earlier back up was required to be used.

Testing of back up tapes is extremely time consuming (typically two days) but a new schedule of testing will be undertaken to reduce the chances of this being an issue in future. From now on, once a quarter, a sample of the backup tapes will be tested. After three iterations of successful testing this will be reduced to six monthly.

It is possible to reduce the amount of time it takes to upload backups through reducing the amount of data stored on our systems. The amount of data being stored is growing rapidly. It is proposed that a programme of staff education and encouragement is devised to manage the data quantity. One option the service has is to automatically archive data from staff's folders after a given period. It is desired that this isn't done until we have a chance to reduce the quantity through encouraging more individual responsibility.

Recommendation 4: Quarterly testing of back up tapes will take place until full confidence is restored in the backup recording and retrieval process. The amount of data on systems is more closely managed through educating staff to take more responsibility for managing their data.

4. Cyber-Attack

Viral and Ransomware attacks

Cyber-attacks and in particular ransomware attacks have been on the increase globally. Recent estimates are that there has been a 400% increase in ransomware attacks since the start of this year. Ransomware attacks are becoming increasingly sophisticated. Those perpetrating these attacks use polymorphic viruses. These constantly evolve to prevent detection by software systems that protect networks from infection.

Our recent experience of these attacks has demonstrated the potential effectiveness of these viruses.

The first level of protection from such attacks is the email and web filters BMKFRS deploy.

Because of the nature and rapid development of viruses it is possible for them to penetrate these filters and find their way into individual's inboxes. Investigation has shown that there is better software for protecting our systems available on the market.

The second level of protection is therefore individuals.

A programme of reminders and education has started to highlight to staff the dangers of viruses and how to recognise suspicious emails and then what to do and what not to do with them.

Recommendation 5: That our first level of protection is enhanced by reconfiguring our existing anti-virus software by introducing stricter software protocols and devoting more processing power to scanning incoming data and website activity to prevent virus penetration. This may reduce system performance to a certain degree. That our current email and web filters are replaced with better software. We are currently awaiting costings from suppliers.

Recommendation 6: The programme of staff engagement and education is continued to ensure they have the best information to enable them to recognise threats.

ICT Health Check

BMKFRS recently had an ICT Health Check undertaken by a firm of consultants. This was commissioned in partnership with OFRS and RBFRS as part of the process for preparing for the Code of Connection for the new Emergency Services Network commissioned as part of the Emergency Service Mobile Communications Programme (ESMCP). The health check was funded by the Central Government Programme Board for the project.

The health check was a very in depth review of the security of our systems based through practical exercises by ICT security experts simulating attempted attacks on our systems. As expected prior to the health check, the exercise revealed a number of potential weakness in our infrastructure and systems. The in depth nature of the findings has given us a degree of confidence in both what they found and also where they weren't able to affect penetrations of our systems.

The consultants provided a very in depth report of every single potential and actual weakness they could expose. The report is in commercial confidence so has not been made available as part of this report. As previously requested legitimately by the ESMCP programme team the report has been copied to them.

It is estimated that the work to rectify these potential weaknesses will take until June 2017. The costs (which are being sought in partnership with BCC) are still being estimated by potential suppliers. The work is prioritised in line with the report's recommendations on risk rating. Much of the critical findings are already rectified.

Recommendation 7: The findings of the ICT Health Check are actioned by the ICT team. Any revenue shortfalls arising from requirements to purchase software upgrades will either be found from in year funding or through contingency and reported through our usual governance frameworks.

5. Summary of Recommendations

- Recommendation 1: That the DR servers are decommissioned and our DR functions are moved to a Cloud provider that satisfies our operating and data security needs. The most suitable option for BMKFRS is a Hot configuration. The budget for this is based on the costings indicated above plus a 25% contingency for unforeseen consultation or system configuration and data requirements. The implementation costs are provided through an in year virement from identified underspends elsewhere in the Service or contingency.
- Recommendation 2: Our network arrangements with BCC, provided through Updata, continue to be satisfactory and should continue for the remainder of the contracted period.
- Recommendation 3: By moving to a Cloud based DR arrangement our single point of failure in having a single data feed into SHQ will be eliminated.
- Recommendation 4: Quarterly testing of back up tapes will take place until full confidence is restored in the backup recording and retrieval process. The amount of data on systems is more closely managed through educating staff to take more responsibility for managing their data.
- Recommendation 5: That our first level of protection is enhanced by reconfiguring our existing anti-virus software by introducing stricter software protocols and devoting more processing power to scanning incoming data and website activity to prevent virus penetration. This may reduce system performance to a certain degree. That our current email and web filters are replaced with better software. We are currently awaiting costings from suppliers.
- Recommendation 6: The programme of staff engagement and education is continued to ensure they have the best information to enable them to recognise threats.
- Recommendation 7: The findings of the ICT Health Check are actioned by the ICT team. Any revenue shortfalls arising from requirements to purchase software upgrades will either be found from in year funding or through contingency and reported through our usual governance frameworks.

6. Conclusion

The ICT team has undertaken an in depth and technical review of some of the significant threats to our ICT infrastructure which is critical to the operation of BMKFRS. As a category 1 responders as defined in the CCA 2004, BMKFRS has a duty to ensure it is able to operate as a high reliability organisation. Therefore the findings and recommendations of this report are designed to ensure that BMKFRS can continue to utilise the latest technology to support its operations at all times.