ADUR & WORTHING
COUNCILS

Joint Governance Committee
31 July 2018
Agenda Item 9

Disaster Recovery (DR) Test and Beyond

Report by the Director for Digital & Resources

Executive Summary

1. Purpose

1.1. This report provides a high-level summary of the results of the DR scenario test (loss of mains power to the data centre) carried out on 16/06/18, with recommendations for improving the DR capability for this particular scenario.

1.2. This report addresses the subject of DR on a wider scale; focusing on other disaster scenarios that have potential to disrupt information technology (IT) services. The report sets out the Council's plans to mitigate these risks and how the planned mitigation and Technology Strategy support the Council's Business Continuity Plans.

1.3. The Committee is requested to acknowledge recommendations for improvements that will ensure the continuation of 'on-premise' IT services in a mains power loss scenario. These recommendations will result in investment to extend the runtime of data centre batteries to 3+ hours and the sourcing of a service to supply temporary power (generator) within 2 hours.

1.4. The Committee is requested to review and comment on the Council's plans to mitigate risks associated with other disaster scenarios. Endorsement in this area will result in an updated Disaster Recovery Strategy that underpins the Council's Business Continuity Plans.

1.5. The Committee is requested to review and comment on the recent incident that affected telecoms services, and the plans to mitigate the impact incident's of this type have on the Council's services.

2. Disaster Recovery Test (16/06/2018) Results & Recommendations

2.1. **Summary:** A disaster recovery exercise was carried out on 16/06/18 focused on recovering IT services operated from the on premise data centre (Town Hall) in the event of mains power loss. The proposal to execute this test was noted in a previous report to JGC on 31/01/18.

2.2. The test confirmed IT services running from the Town Hall can continue to operate on generator-power. However, it also highlighted the complexity & risk of automating the system shutdown and that, in a live scenario, personnel with specific skill sets would need to be available 24x7x365 to recover services promptly, which is not a viable option.

2.3. **As a result of the test, the recommendation to improve the DR capability for this scenario is to maintain constant power to the Town Hall data centre, which can be achieved with new batteries in data centre power systems and a more immediate generator delivery timescale.**

2.4. **Power Down:** The test commenced at 07:30 with 15 personnel (10 internal and 5 external contractors). At 08:30 the mains power was switched off and the data centre power systems began an automated shutdown 6 minutes from power being withdrawn. The data centre power systems shut down 90% of the environment, but failed to shut down all systems. After 1 hour of running on batteries, the on-site team intervened to shut down the remaining systems manually.

2.5. **Temporary Power:** Generator power was introduced at 10:00. The initial attempt failed, but the issue was promptly identified as a modified cable (supplied by the generator hire company) and a subsequent test demonstrated a stable power supply to data centre environment. Following a short period of running on generator power, mains power was introduced seamlessly and the generator was turned off and made ready for collection.

2.6. **Testing:** Technical infrastructure & application and business application tests commenced at 10:00, completing at 15:30 when communications were sent to stakeholders to confirm services were available.

2.7. **Issues:** As a result of the system shutdown there were issues with the Worthing revenues & benefits system and with load-balancing the virtual server environment (VMWare).

2.7.1. The cause of the issue with the revenues & benefits system was a configuration file that had incorrect settings and this was remedied promptly during testing on 16/06/18. The details of this issue (and fix) have been documented to aid a prompt recovery should it recur in the future.

2.7.2. The load-balancing issue in the VMWare environment slowed down access to some systems on 18/06/18 but was mitigated by closing down unnecessary services.

2.7.3. A support call with VMWare on 18/06/18 guided the team to a full resolution at 15:00 on the same day. It is not possible to identify the exact cause, but it's reasonable to suspect the automated shutdown process due to its partial failure to shut all systems down in a controlled manner.

2.8. **Conclusion & Recommendations:** There is risk associated with operating line of business applications & systems from the Town Hall i.e. the Council's are reliant on physical hardware at the Town Hall. Whilst this DR 'scenario test' addressed power loss, there are several other risks that are still apparent e.g. fire or flood, that pose a risk with the current 'on-premise' operating model.

2.9. The plan to mitigate these risks is to host systems and services with cloud service providers in resilient, stable, and secure environments. Services such as Google, MATs and Salesforce already operate in this way and the in-flight cloud migration project (IaaS) will result in the shift of services to Amazon (AWS) over the next 12-18 months.

2.10. Because there is an active project tasked with mitigating these risks, the response to this recent DR scenario test needs to be balanced, giving consideration to the long-term plan.

2.11. The automated shutdown process caused issues i.e. systems did not automatically shut down in full. The process of shutting down systems in full resulted in issues with the Worthing Revenues & Benefits system and the load-balancing function on the virtual server environment. The impact of these issues was mitigated by the presence of a multi-skilled

on-site team, but this is unlikely to be the case in a live scenario and the impact could have therefore been more severe. These issues demonstrated the automated shutdown process would not be viable without significant cost to ensure people with the relevant skills were available 24x7x365.

2.12. The shutdown of systems was intended as an intermediary until the generator arrived to power the data centre, enabling services to be made available. Given the issues the shutdown caused, it makes sense to focus on maintaining constant power to the data centre.

2.13. We plan to invest in new batteries to extend the runtime of the data centre power units to 180 minutes and source improved timescales for the delivery of a generator that aligns with the new battery runtime capability.

2.13.1. This will ensure the Council's, subject to out of hours on-call arrangements, have the capability to maintain power to the data centre in the event of a mains power outage.

3. Risks to Council Information Technology (IT) Services

3.1. The first part of this report focused on the outcomes of a test to recover IT services in the event of mains power loss to the on-premise data centre at the Town Hall. This section reviews other areas of risk to IT services and sets out the Council's plans to mitigate these risks.

3.2. **Risk of Fire, Flood, Theft, Power & Hardware Failure:** There are several 'disaster' scenarios that present risk to the operation of IT services. These risks can be grouped as 'physical' as they all relate directly to the on-premise nature of the current operating model. Scenarios such as severe fire, flood, theft, power or hardware failure could prevent the Council's from operating their IT services from the Town Hall, and the full recovery of services could take between 2-4 weeks; potentially requiring the procurement of hardware and the recovery of systems and/or data from disk or tape backup.

Mitigation Plan

3.2.1. Business critical services such as Google (email, calendar, storage) MATs, and Salesforce already operate from cloud service providers and are therefore not reliant on the Town Hall. There is an in-flight cloud migration project (IaaS), which is

tasked with moving services away from the Town Hall to Amazon (AWS), who are a cloud hosting provider.

3.2.2. The AWS environment is already operational, with some key underpinning services running and some business applications replicated and in test. The resilient (dual) network connections have been ordered and, when in place, the migration of more business applications will commence. The migration of services from the Town Hall is expected to complete over the next 12-18 months, which will mitigate the impact of fire, flood, theft, or hardware and power failure significantly.

3.2.3. Google services, which are already running email, calendar, and storage services for the Council's, will be expanded to become the main storage repository. As part of the IaaS project, the Council's will close down servers running data storage services (file shares) and move data to the Google environment. This migration activity is underway now and is expected to complete within 8 months, further mitigating the impact of a fire, flood, theft, hardware or power failure.

3.2.4. The recovery from mains power failure at the Town Hall data centre was tested on 16/06/18. The test confirmed services can continue to operate on generator-power, but also demonstrated the automated shutdown approach was complex & unreliable, thus putting physical equipment at risk. The mitigation plan for power failure is to invest in new batteries to provide improved battery runtime, and to source improved generator delivery timescales to ensure services operated from the Town Hall receive a constant power supply.

3.3. Risk of Cyber Attack: The Council's, like most organisations in the modern world, are at risk from cyber attacks. These risks are present regardless of where services operate from (cloud or on-premise) and mitigating these risks requires an ongoing process of protecting systems through applying software & security updates as vulnerabilities materialise. Cyber attacks can take many forms, from Malware; malicious code with intent to steal or destroy data, to Denial of Service (DoS) attacks, which flood systems with traffic to prevent operation.

Mitigation Plan

3.3.1. **Security Updates:** The Councils apply security patches to Microsoft servers monthly, with the exception of emergency patches, which are applied immediately. As systems and services are migrated to AWS, the security updates to Microsoft servers will be carried out by the managed service provider. The approach to security updates for servers in AWS will be reviewed as they migrate to ensure systems are updated aggressively without degrading application performance. Security updates for technologies such as Adobe, Apache Tomcat, VMWare, and firewalls are reviewed regularly & applied where the risk is high.

3.3.2. **Annual IT Health Check:** The Councils have an active Public Services Network (PSN) circuit for access to Government services. The compliance certification for PSN requires annual IT health checks carried out by CREST-approved independent organisations. These health checks capture any vulnerabilities or issues that have not been identified or closed through security updates from vendors.

3.3.3. The health check involves internal & external penetration testing and vulnerability assessment of the Council's networks & servers. The results of this exercise are submitted to the Cabinet Office for assessment and approval prior to certification being awarded.

3.3.4. **Secure Design:** The cloud migration project (IaaS) will shift servers to AWS over the next 12-18 months. The approach to AWS security differs from the current (on-premise) model i.e. each application is ring-fenced in a private cloud within the Council's private environment (tenancy). By default, each server is unable to communicate with resources that sit outside of its private cloud (even Council resources). As part of the migration, rules will be applied to allow only essential communication to other servers, networks, or resources.

3.3.5. This AWS approach to design reduces the 'blast zone' and mitigates the potential impact of cyber attacks because they often attempt to spread across internal servers or networks once the perimeter network has been penetrated.

3.3.6. **Spread Portfolio:** The Technology Strategy and the approach to its delivery mitigates the impact of cyber attacks. The move to cloud service providers is being carried out using several providers; MATs, Amazon (AWS), Google, and Salesforce. This spread of cloud service providers limits the potential impact a cyber attack or other disasters may have because it's very unlikely that multiple service providers will be affected.

3.3.7. **Single Sign-On:** The Councils will be reviewing the approach for authentication to cloud services to mitigate the risk of unauthorised access. Currently, authentication to each cloud service requires a separate password. This prevents the practical implementation of consistent password formats & forcing cyclical password changes. Furthermore, where personal devices are used, there is risk that passwords to cloud services are retained locally on devices (cached), presenting risk of unauthorised access.

3.3.8. The Councils will be assessing the options and costs to implement a single sign-on service where access to the cloud services will be controlled; forcing a consistent password format across the Council's networks, its cloud services, and forcing authentication to mitigate the risk of unauthorised access.

3.3.9. **Mobile Device Management (MDM):** Council laptops and mobile phones currently have encryption with a standard MDM service through Google (phones) and Microsoft encryption on Council-owned laptops. The Councils will be reviewing the options for a single MDM service that encrypts devices and provides greater levels of control over personal devices to mitigate unauthorised access and protect Council data.

4. Council Telecommunications Services

4.1. Telecommunications Issues - Background

4.2. Over the last year there have been intermittent stability issues with the Councils' telecommunications service (Avaya), manifesting as call drop-out's and loss of 'presence' on the back-office phones. These issues were raised with the incumbent supplier on several occasions, along with requests to get call recording to auto-pause recording for the exchange of payment card details.

4.3. The incumbent supplier was given several opportunities to address these issues, but failed to do so, resulting in a loss of confidence and the Council's executing a process to onboard a new supplier. Through liaising with Avaya, five 'recommended' suppliers were identified and in June 2018 a 'preferred supplier' was selected. The transition to the new supplier commenced, aiming to complete towards the end of July 2018, but the previous 'intermittent' issues worsened significantly resulting in the acceleration to allocate control to the new supplier.

4.4. Telecommunications Services - Major Issues

4.5. On Monday 25th June, whilst the transition plan was being executed to transfer control of telecoms services to the new supplier, the stability of the telecoms service degraded severely with a total system loss that resulted in no inbound or outbound calls. In response, the process to transition control to the new supplier was accelerated. The new supplier began to assess the systems, but due to the continuation of the issue, the disaster recovery (DR) service was commissioned. Physical DR telephone handsets were deployed in the Contact Centre, and the main switchboard and 'gold' numbers were diverted from Tuesday and remained diverted until Thursday 28th June.

4.6. With the main switchboard and 'gold' numbers routing through the DR telecoms service, the handover process to the new supplier continued to further empower them to resolve the issue with Avaya. On Thursday 28th June, the outgoing supplier reported the Avaya system appeared stable, resulting in the process of switching back to the Avaya. The Avaya system remained stable for the remainder of the week.

4.7. On Thursday 28th June final handover details were passed to the new supplier, who were then able to perform detailed investigations. The

following Monday (2nd July), the Avaya system became inaccessible once again. At 10:00, in agreement with the new supplier, the decision was made to commission the DR telecoms service, which was complete by midday with calls to the switchboard and 'gold' numbers routing through the DR telephony service.

4.8. The new supplier, who, following further investigation, recommended the complete rebuild of the Avaya system due to severe instability. The new supplier worked through the remainder of the week and weekend to rebuild the Avaya system, which was confirmed as 'ready for operation' on Sunday 8th July. On Monday 9th July, the new supplier attended the Council's premises to support the switch from the DR telephony system to the newly built Avaya system.

4.9. By 15:00 on 9th July 2018, the main switchboard and 'gold' numbers were routing through the new Avaya system and the new supplier monitored the system closely as call volumes increased.

4.10. **Mitigation Plan:** Telecommunications services are business critical as they're the main method customer's use to contact the Councils. The primary focus is ensuring stability is maintained on the Avaya system. During the supplier selection process, the new supplier was made aware of intermittent stability issues, but were called to respond to a catastrophic situation with urgency, and responded well.

4.11. Once the primary 'newly built' Avaya system is demonstrably stable, the Councils will work with the supplier to form a <u>new</u> DR solution that can be brought into action quickly without the need to divert numbers. Invocation tests will be scheduled periodically to ensure the DR solution delivers acceptable continuity of service.

4.12. Research will be carried out to identify the options, benefits and costs of moving to cloud-telephony to deliver an 'access from anywhere' service that is highly scalable, robust, and resilient.

5. Business Continuity & Technology Strategy

5.1. Part of the Technology Strategy is to shift from traditional, on-premise services to cloud services. This has already been applied in part with the adoption of Google services for email, calendar, and storage, MATs as the default platform for new/redesigned digital services, and Salesforce as the Customer Relationship Management (CRM) system. Over the next 12 months, more services will be moved to cloud service providers with the shift of services running on physical servers to Amazon (AWS), and further development & digitisation of applications on MATs.

5.2. The aim of the cloud migration project (IaaS) is to move all 'line of business' applications to cloud service providers, thus removing any reliance on the Town Hall apart from it being a place of work (i.e. office space).

5.3. Research will be carried out on options, costs, and benefits of true cloud-based telecoms services. It should be noted that the telephony issues referenced in section 4 were not as a result of on-premise services. The issue derives from poor configuration by the supplier that implemented the solution, who are currently being exited.

5.4. Research will be carried out on the options and costs for strengthening security for remote access to services e.g. mobile device management (MDM) and a single-sign on portal to support the prevention of unauthorised access without making access too complicated.

5.5. The Technology Strategy supports the Councils' Business Continuity Plans by shifting to services that are accessible from anywhere with an Internet connection. This approach will be strengthened by the Gigabit Project that will deliver Internet connections at Council premises that are independent of the Town Hall.

6. Engagement and Communication

6.1. This report has been formed collaboratively by internal Council staff that are involved in information technology, business continuity, and customer services.

7. Financial Implications

7.1. The plan to improve the DR capability for the 'disaster scenario' of mains power loss to the data centre is expected to cost ~£10K. This will cover the replacement of old batteries in the data centre power systems and a potential standing charge to have a generator on site within 2 hours. Whilst this exceeds the budget for data centre maintenance, existing budgets should cover these costs.

7.2. The cost for shift of services to Amazon to mitigate the impact of risks associated with the on-premise IT operating model are covered by existing revenue budgets. The sections addressing 'other risks' and how these will be mitigated in the future may require funding e.g. single sign-on and MDM, but proposals will be put forward when appropriate solutions have been sourced and the costs are known.

8. Legal Implications

8.1. There are no legal implications as a result of the contents of this report.

Background Papers

Disaster Recovery Test - JGC Report (30/01/2018)
Technology Strategy

Officer Contact Details:

Name: Robert Wood
Role: ICT & Digital Services Manager
Telephone: 07736 597499
Email: Robert.wood@adur-worthing.gov.uk

Sustainability & Risk Assessment

1. Economic

- Matter considered and no issues identified.

2. Social

2.1 Social Value

- Matter considered and no issues identified.

2.2 Equality Issues

- Matter considered and no issues identified.

2.3 Community Safety Issues (Section 17)

- Matter considered and no issues identified.

2.4 Human Rights Issues

- Matter considered and no issues identified.

3. Environmental

- Matter considered and no issues identified.

4. Governance

- This report sets out the Councils approach to managing risk associated with Information Technology services which are critical to service delivery and the Councils reputation. These risks are managed and reviewed on a continuous basis.