

22-10-2018

Mangaung Metropolitan
Municipality



MANGAUNG

METRO MUNICIPALITY
METRO MUNISIPALITEIT
LEKGOTLA LA MOTSE

DIRECTORATE
CORPORATE SERVICES

ICT Sub-Directorate

Date: 15 October 2018

ITEM FOR COUNCIL

THE SPEAKER

ICT DISASTER RECOVERY REPORT: CRISIS EVENT DURING JULY AND AUGUST 2018

1. PURPOSE

The purpose of this report is to advise and provide feedback to the Council of the IT Disaster Management and Recovery measures implemented and executed during the crisis that affected all IT related Systems during the month of July and early August 2018.

2. BACKGROUND

On Thursday, 5th July 2018 the Bram Fischer Building evidently as confirmed, experienced approximately five (5) consecutive power failures/interruptions. These events/incidents have been described by our IT Infrastructure Unit as extremely irregular and unpredicted. After alerting Facilities Management of this troublesome predicament, the preliminary investigation by the Facilities Management Unit revealed that one of the main electrical circuit breakers in the Bram Fischer Building was demonstrating symptoms of malfunctioning. This faulty circuit breaker is an automatically operated electrical switch designed to protect an electrical circuit from damage caused by excess current from an overload or short circuit. Its basic function is to interrupt current flow after a fault is detected.

Furthermore, these problematic electrical circumstances persisted throughout the weekend with electricity continuously travelling through the faulty circuit breaker providing improper, unregulated electricity throughout the Bram Fischer Building which includes our IT Server room in the basement. This problem however could not be attended to due to unavailability of an electrician and this problematical circuit breaker was only repaired/replaced on Monday, 9th July 2018 by a qualified electrician. Our IT Infrastructure Unit only discovered the extent of the dilemma on Monday, 9th July 2018 and alerted the severity and the implications thereof affecting all IT Systems

and the Collapse of the Server Hardware on Tuesday, 10th July 2018. It is clearly conceivable that this faulty circuit breaker inadvertently led to the collapse of all IT Systems and the Collapse of the Server Hardware as experienced during the mentioned period.

3. DISCUSSION OF ACTIONS & INTERVENTIONS EFFECTED

The following actions were immediately initiated to resolve the predicament:

- Action 1 – [Offsite Remote Access]: Our contractual authorised Service Provider was rapidly notified and given remote access to gain admittance into our Computer Server environment from a remote location. This allowed BCX (Formerly Business Connexion) to work offsite from Johannesburg and determine the gravity and remedial action while inspecting our Server computers and network infrastructure. The main intention of accessing the Server Computer remotely was to analyse our data integrity, determine if any errors occurred and then reboot the main host. This effort did not produce any successful results and corrective engagements where not effective.
- Action 2 – [Onsite Physical Attendance]: As a result of the failure suffered via remote access and the issues have not been cleared, BCX was requested to urgently avail themselves to assist the Municipality. BCX arrived from Johannesburg during the night of 10th July 2018. Shortly after arriving in Mangaung, BCX worked through the night and early morning until the next day afternoon attempting to remedy the crisis and reboot the Server. These efforts did not generate any fruitful results and counteractive actions where not useful.
- Action 3 – [Commandeering the Backup Server]: On Thursday, 12th July 2018 the IT Infrastructure Unit endeavoured to reboot the Backup Computer Server located on the premises of the Fresh Produce Market. While in discussions to find possible intermediate solutions with BCX, the IT Infrastructure Unit considered rebooting and utilising this Backup Server with an understanding that some Municipal Systems and Network functionality would be available temporarily although limited and very slow. BCX considerably cautioned the municipality that rebooting the Backup Computer Server located on the premises of the Fresh Produce Market without first analysing and securing the existing data on the main host server may lead to a more catastrophic scenario involving permanent data loss and file corruption if unsuccessful. These drastic measures were suspended until the municipality could obtain a comprehensive system analysis before processes would be undertaken.
- Action 4 – [Escalation to Expert Specialists]: The complications were further escalated to the distinctive concerned designers and manufacturers of our Computer Servers DELL EMC (EMC). EMC were requested to

81

remotely connect and analyse the data for errors. This was a very delicate and meticulously process that lasted until Sunday, 14th July 2018. EMC were not able to produce any successful results.

- Action 5 – [Escalation to Data Recovery Service Provider]: The physical files were taken to data recovery specialists LVC in Pretoria on Tuesday, the 17th July 2018 for analysis of any errors. The analysis revealed that the mother board of the main host server was damaged due to unusual power surge. The data array and the damaged discs were scanned and rebuild by LVC.
- Action 6 – [Data Recovery & Server restoration]: The Main Host Server was delivered to MMM on Wednesday, 18th July 2018 with immediate execution of data recovery procedures and hardware reconnection. Delivery of additional new Hard Disk Drives realised. During the reconnection process of the hardware, a further discovery was made regarding the compatibility (hard coded security measures within the hardware itself) of the serial numbers of the new Hard Disk Drives. These hardware components do not simply get plugged in and start to function immediately, they have built in hard coded security measures within the hardware itself and these are designed to prevent any data leakages as a security feature. These Hard Disk Drives were not authentically recognised as “friendly” by the main host server and therefore access to our data could not be made.
- Action 7 – [Rewrite and Reconfigure Hardware]: An engineering process was undertaken to rewrite and reconfigure the serial numbers to be read by the server. The server was restored with the PayDay system on Thursday, 26th July 2018. The Solar Financial System was restored on Saturday, 28th July 2018 together with our e-mail Servers and other systems. All municipal data is now accessible and all Systems operational. The service provider concluded with feedback that no data has been lost or corrupted. During these activities the backup server at our Fresh Produce Market has also been restored.
- Although some services including financial reporting data were restored later than anticipated, no data loss has been experienced by the municipality
- On the 17/08/18. Data year end data was verified to 4 AM 10 July
- All subsequent data up to date was successfully restored.

4. CONTINGENCY PLAN DURING THE DISASTER PLAN

A multidisciplinary team was established to deal with an overarching contingency plan to mitigate the effects of the collapse of our systems and ensure a semblance of continuity of our operations albeit that most would be at a significantly slow and hard manual way. The following were key elements of the plan:

4.1. Communications Plan (Localised)



- a) Electronic and Print Media (communication with both our internal and external stakeholders) has been implemented;
- b) Alternative Temporary Email Accounts have been created; and
- c) Social Media Platform (Create a Temporary WhatsApp Groups) have also been created.

The main idea was that communication should inform stakeholders of all relevant issues including payment channels available during this period.

4.2. Operational Plan

- a) Revenue Collection (Communication to the effect that Payment of Services by manual operation at directed pay points, EFT; Easy Pay and UltiPay remains available);
- b) Payment of Creditors (Communication to the effect that Payment of Creditors would not be affected); and
- c) Payment of Salaries (A Plan for Manual Payment of Salaries has been developed in conjunction with ABSA Bank). The process started once the event of the system was not fully restored to normal functionality by the 20th July 2018. Payment of salaries was ultimately done manually on the 26 July 2018.

5. CONSEQUENCE MANAGEMENT

- 5.1. Throughout this experience or process of server collapse, greater emphasis, urgent priority and attention was placed on the restoration of the functionality of our server which was eventually achieved on the morning of July 26, 2018 at around 02:30am.
- 5.2. It follows from this that greater emphasis, urgent priority and attention will now shift to the commissioning of a detailed investigation whose report will inform our way forward and where appropriate, consequence management will also take effect. A service provider has been appointed to determine the exact cause, the circumstances and recommendations. An investigation report to this effect is pending.

6. LESSONS LEARNT

- 6.1 The following lessons have been learned:
 - 6.1.1 ICT Sub Directorate should play a central role in the procurement and maintenance of all ICT Systems. Some ICT systems are currently not managed and maintained by the ICT Sub Directorate.
 - 6.1.2 The maintenance plan and agreement should be in place and updated regularly.
 - 6.1.3 The ICT Server Infrastructure has reached ICTs life cycle and requires urgent attention.
 - 6.1.4 The budget of ICT is insufficient to respond to the current infrastructural challenges and introduce modern ICT Systems and service delivery platforms. The ICT Governance Framework is not adequate to escalate the importance of ICT at all levels.
 - 6.1.5 The ICT Human Resources needs continuous capacity building to align with modern day technological advances and be able to better respond to ICT business continuity and data security disaster.

7. PLANNED ACTION

- a) Procurement and maintenance of all ICT related Systems must henceforth be done by ICT using budget of user departments;
- b) Immediate recovery of data and back for interim period of 12 months whilst tender for data centre upgrade is in progress;
- c) The budget of ICT be reviewed and adjusted to affirm ICT's central role in terms operations and optimising service delivery;
- d) ICT governance be standing be agenda to EMT and MAYCO;
- e) A special training and capacity building program be introduced by the Directorate: Corporate Services to upskill relevant ICT staff;
- f) Urgently undertake ICT Environment, Systems and Infrastructure Audit/Review;
- g) The ICT policies, Business Continuity, Disaster Recovery and Operational Plans be urgently reviewed or grafted;
- h) Back up and cloud environment strategy and plan be made immediately;
- i) Carry out comprehensive investigation on the collapse of the server.

8. PROGRESS ON PLANNED ACTION

8.1. Recovery of data

(BCX) was appointed in 2012 by the municipality for the procurement and installation of servers situated in Bram Fischer Building, Free State Stadium and Fresh Produce Market. The purpose for the procurement was primarily for the financial system SOLAR. BCX is the initial service provider that designed and installed the entire infrastructure for Mangaung Metropolitan Municipality's data centres.

For continuation of services and remedial action Mangaung has entered into an agreement with BCX for the service provider to assist with storage, network and software related issues.

The Maintenance and service level agreements with BCX for the current infrastructure, restoration and updated architecture has been completed which includes a backup data centre at Freshmark and additional live replication. In total MMM currently has 3 lives data centres in operation with appropriate SLAs and maintenance in place for the interim period of 12 months ending August 2019. Tender specifications have been developed for a long-term upgrade of data centre.

8.2. Financial implications for data recovery and back up

Description	Duration	Amount
HPE Switches: maintenance and replacement of faulty switches, this needs to be done before recertification of our environment.	12 Months	R26 277.02
HPE Server: maintenance and replacement of faulty switches, this needs to be done before recertification of our environment.	12 Months	R172 872.60
Recertification – Unified NVX: for the Vendor to renew insurance on the current equipment, a process of recertification is critical; this will allow a view of any issues and risks that need to be rectified before our hardware is insured.	Once Off	R116 815.83
VM Ware Renewal: the entire server architecture is built on VM Ware, it is critical to have support and maintenance for our virtual environment.	12 Months	R104 495.58
Veeam Renewal: Veeam Backup & Replication is a data protection software for all our backups and replication within our environment. SLAs and licensing a critical to the functioning of the backups, without which the vendor cannot verify the backups of our servers.	12 Months	R377 742.57
EMC Support Services: for vendor warranty and support on the current hardware, this is a critical service in case of hardware failures	12 Months	R218 960.00
Move VNX and Recover points: the procedures require engineering expertise to replicate all the current data as a once off operation. Thereafter incremental backups will continue as normal.	Once Off	R193,718.65
HPE Tape Library: critical for offsite storage as the current design only backs up onsite.	Once Off	R 190 925,92
Firewall Upgrade: the current firewall is part of the original architecture design by BCX, it is reaching end of life and will not be able to support the currently upgraded links for the Fresh Produce Market Datacentre as the console monitor's QOS (Quality of Service) and any threats both internally and externally that might affect the servers.	Once Off	R901,355.17
Data Recovery: for services rendered to restore the current servers	Once Off	R103 702.68
BCX Site Inspection: for correction and alignment of our backup connectivity links.	Once Off	R33 337.47
Total		R2 440 203.49

The intervention was procured through deviation procedures of the Supply Chain Management.

8.3. Budget Review

A process for budget review and realignment has begun. This will include investigation on indicative budget for the three-year budget for normalising the ITC environment.

8.4. ICT governance

A tender advertisement has been approved for the panel of service providers to assist and support the municipality in the urgent review and audit of ICT Environment, Systems and Infrastructure, ICT policies, Business Continuity, Cyber Security, Disaster Recovery and Operational Plans. ICT will officially feature in the EMT meetings and its recommended that it features in the Mayoral Committee.

8.5. Capacity building upskilling of ICT Staff

More ICT interns and appropriately qualified ICT staff will be recruited. Staff is receiving ongoing training and upskilling through attendance to workshops and conferences. A study programme is being developed to develop existing staff in the next year.

8.6. Integration of Systems and Call Centres

A process for integrating systems and call centres has begun to enhance service delivery.

9. RECOMMENDATION AND PROGRESS UPDATE


- a) The Council takes note of the IT Disaster Management and Recovery measures implemented and executed during the crisis that affected all IT related Systems during the month of July and early August 2018.
- b) The Council takes note of the planned action and progress made on paragraphs 7 and 8 of the report.
- c) Council takes note of this report and final report pending investigation report be tabled to council.

Submitted by:



D. S. R Nkaiseng
Head: Corporate Services
Date _____

Recommended by:



Adv. T B Mea
City Manager
Date 24/10/2018

Approved By:



Cllr S M Mlamleli
Executive Mayor
24/10/2018

