

**Manchester City Council
Report for Resolution**

Report To: Resources and Government Overview and Scrutiny
Committee – 18 June 2009

Subject: Service interruption resulting from ICT disruption in
February 2009.

Report of: Geoff Little, Deputy Chief Executive (Performance)
Elaine Bowker, Director,
Manchester Improvement Programme

Summary

In Dec 08 a virus known as 'Mario Forever' was found to exist on MCC networks and PCs followed in early January 2009 by a more serious virus known as 'Conficker' or 'Downadump' or 'Kido' being detected.

The incident was managed within the Corporate Business Continuity Framework. The incident was effectively managed and there were no significant failures in the provision of services to the public. The response to the incident has been reviewed and lessons learnt have been identified and are now being taken forward.

The aim of this report is to provide an overview account of this ICT virus incident and draw out the key recommendations to improve both corporate business continuity and our ICT network in order to enhance Council resilience and thus strengthen the capacity to respond to any further incidents in the future.

Recommendations

The Committee are asked to note the response to the ICT virus and the recommendations set out to improve future resilience.

Wards Affected:

All

Contact Officers:

Name: Elaine Bowker
Position: Director, Manchester Improvement Programme
Telephone: 0161 219 6958
E-mail: e.bowker@manchester.gov.uk

Name: Geoff Little
Position: Deputy Chief Executive (Performance)
Telephone: 0161 234 3280
E-mail: g.little@manchester.gov.uk

Name: Steve Park
Position: Strategic Head of ICT (*interim*)
Telephone: 0161 277 5921
E-mail: s.park@manchester.gov.uk

Name: Fiona Worrall
Position: Head of Business Support, Neighbourhood Services
Telephone: 0161 234 3926
E-mail: fiona.worrall@manchester.gov.uk

1.0 Introduction

- 1.1 The recent virus within the ICT estate gradually led to impacts across the Council's services, eventually causing significant disruption and warranting the invocation of the Corporate Business Continuity Plan.
- 1.2 The subsequent crisis management arrangements to respond to the incident, the need to ensure essential activities and services are maintained and to guide the recovery process to the "business as usual" norm was led by an Emergency Management Team (EMT).
- 1.3 The incident highlighted that awareness and understanding of Business Continuity processes and crisis management procedures were not consistent across the organisation. However, clear and strong management principles were evident and any clarity / specialist advice was in provided by the Civil Contingencies Unit (CCU), where required
- 1.4 The aim of this report is to provide an early account of the ICT virus incident draw out and embed the lessons to improve corporate business continuity in order to enhance Council resilience and thus strengthen the capacity to respond to any further incidents in the future.

2.0 Incident Background

- 2.1 On 4 Dec 08 a virus known as 'Mario Forever' was found to exist on MCC networks and PCs. Our anti-virus supplier, subsequently provided an anti-virus update to fix the virus which was implemented across the ICT estate. On 9th January 2009, a more serious virus known as 'Conficker' or 'Downadump' or 'Kido' was detected on MCC networks and PCs.
- 2.2 Whilst the initial virus, 'Mario Forever' was beginning to come under some degree of control the second virus, 'Conficker', was starting to impact PC users in terms of system performance and then total unavailability of systems. To address this both our anti virus and our desktop PC providers developed a solution to attempt to alleviate the impact of the virus and to put in place steps to eradicate it from our ICT estate.
- 2.3 The success of this was been clearly limited as the ICT estate continued to experience serious performance problems. During February, the virus gained access to several key servers resulting in all users suffering performance problems.
- 2.4 The virus was specifically designed to exploit Microsoft IT systems and Microsoft had recently been successful in resolving the same issue at Wakefield MBC. A Microsoft technical manager joined the ICT Service to develop emergency measures to tackle the virus.
- 2.5 The conclusion of this rapid assessment was that highly skilled technical resource needed to be secured immediately to ensure that the network and PCs were brought up to date with the latest security software and administrator passwords and to ensure that we had the appropriate skills to deal with the virus.
- 2.6 The ICT Service addressed the outbreak of the Conficker virus on several fronts:

2.6.1 Intrusion Prevention System (IPS).

The Conficker virus attacks ICT systems by what is known as a "denial of service attack". This means that network traffic is increased and servers are put under excessive pressure to the point where the whole system gradually becomes unusable. A standard measure to help prevent this from happening is the installation of an Intrusion Prevention System which helps repel such attacks. The ICT Service installed such a system at the end of February which had a positive effect on the damage that the virus was causing.

2.6.2 Kaspersky Anti-virus Installations.

Early investigations noted that different types of anti-virus were not installed on different desktop PCs and laptops. An anti-virus management system was installed that allowed the ICT Service to identify how many PCs and laptops

had the correct version of anti-virus installed and more importantly which had not. This allowed the work of the ICT Service to be more focused.

2.6.3 Microsoft Updates (known as patches).

The Conficker virus exploits PCs and laptops that do not have the latest Microsoft patches installed. A system was implemented that ensures that all PCs and laptops (when connected to the network) automatically receive the latest updates which, when coupled with up to date anti-virus software, offer the maximum protection.

2.6.4 Thin-Client Terminals.

Thin-client terminals, also known as Wyse terminals, offer the greatest protection to the Council from ICT viruses since all data is held on the network and not on the PC itself. The ICT Service placed an order for over 2000 Wyse terminals to maximise the level of coverage of such devices across the estate.

2.6.4 Prohibited use of USB Memory Sticks.

The Conficker virus is widely reported to be first introduced into corporate networks of other organisations via the use of USB memory sticks. The use of such mobile media has increased dramatically in recent years and since they generally do not have anti-virus software installed then their continued use poses the largest threat to the Council's ICT systems. It is becoming good practice across the ICT industry to refrain from using such devices where possible. As a result, the ICT Service with the support of the Chief Executive prohibited the use of USB memory sticks and disabled all USB ports on PCs and laptops. Users were assisted to consider and develop new ways of working to remove the need for a USB device through a dedicated help line and support team.

2.6.5 Laptop Surgery

It was important that the Council's laptop PC estate was cleansed of the virus before they were plugged into the Council's network and risked further infection. A laptop surgery was established by the ICT Service in the Town Hall complex that eventually cleaned over 1000 laptops.

3.0 Scope

3.1 Crisis Management

3.1.1 The Emergency Management Team (EMT) first met on 23rd February 2009 after the Corporate Business Continuity Plan was invoked and Incident Level 3 established. The EMT provided a focus for collective updates, advice, direction and co-ordinated action across the Council's Departments.

3.1.2 Clarity on the EMT membership at the outset and the ability to remain flexible in order to involve pertinent individuals as the challenges change is important.

The EMT stood down on 3rd April and the Incident Level was reduced to 2, with a sound crisis management structure still in place to monitor the final progress to “business as usual” and capacity to escalate quickly, if required. The incident is now closed.

3.1.3 Elected Members and Chief Executive and the strategic management team and were kept informed appropriately.

3.1.4 Firm organisation and administrative support was provided by the Civil Contingencies Unit (CCU).

3.1.5 Lessons:

- The business impact revolved primarily around service level degradation both in terms of efficiency and quality of output. This impact was most acutely evident in front line customer facing services. Internal workflow and communication flows were comprised. The response therefore needed a good understanding of the internal dependencies between functions to be considered in more depth by the organisation.
- The impact was been widespread affected all services to varying degrees. Due to the nature of the incident, it presented itself as a creep event initially exhibiting low level, yet pervasive impact across the organisation. As the incident developed, impacts compounded through continued denial of systems access. Localised impacts (in terms of financial loss, reputation impact, breach of regulatory/statutory requirements, threat to human welfare and impact to strategic direction) cumulatively presented a significant threat to the organisation as a whole.
- The Business Continuity System was successful in that there were no major individual breaches of service delivery. However, during the incident major concerns which had to be managed, involved the ability to deliver Council Tax and Business Rates bills, impact to the school admissions decisions making process and notifications, liability claims resultant of impact to customers such as taxi drivers lost earnings, deadlines surrounding year end reporting and grant claiming procedures, and risk to vulnerable adults and children through degraded social care activity.

3.2 Corporate Business Continuity

3.2.1 The Council has a Corporate Business Continuity Plan¹, which has not been invoked over the previous 18 months. This provided the framework for maintaining the Council’s essential services and a flexible structure from which to manage the response and recovery. Outlined roles and responsibilities, crisis management objectives and issues, including EMT membership appear sound.

¹ 2007 and currently under review for updating 09 (delayed due to Incident).

3.2.2 A planned review of the Business Continuity arrangements was already underway with a completion of Mar 09. However as a result of this incident the review has been delayed to enable a more detailed response and to enable us to embed lessons from this incident. This will now be continued and completed by early summer.

3.2.3 **Lessons**

- The incident highlighted that awareness and understanding of Business Continuity processes and crisis management procedures were not consistent across the organisation. However, clear and strong management principles were evident and any clarity / specialist advice was provided from the Civil Contingencies Unit (CCU), if required.
- The evidence suggests more effort is required to embed the business continuity culture corporately and raise awareness across the whole organisation.

3.2.4 There is evidence that the Corporate Business Continuity Plan and supporting structures should have been activated earlier. This would have allowed the potential impacts on service to be understood at an earlier stage. The incident highlighted the importance of support services upon front-line services depending on having strong business continuity and resilience planning.

3.3 **Crisis Communications**

3.3.1 Communications was a significant component of the response, led by the EMT. Members, staff and external partners were kept updated from a corporate perspective. Corporate communications must continue to use specialist or departmental representatives to ensure accuracy and maintain a regular flow of information.

3.3.2 A whole organisation communications initiative was utilised to instruct all staff on “do and do not” regarding ICT procedures and to keep people up to date on progress. This process will need to be made more robust for future incidents. Communications have to be put place at short notice and where necessary to use alternative forms of communication including face to face.

3.3.3 The Strategic Head of ICT issued several communications to all Council staff to provide updates on progress and actions that staff should follow help eradicate the virus.

3.3.4 Good communications with SMT and Elected Members remained throughout including regular updates to SMT briefings to key Members.

3.3.5 External messages were created for all external partners and suppliers which were forwarded to managers to ensure unity of message across the whole organisation. The public were made aware and advice and lines for customer facing services were put in place. Media interest was minimal. Our

communications with regulatory bodies was varied and for the future it will be helpful for managers to consider this as part of the business impact analysis.

3.4 Service Level Business Continuity

3.4.1 The CBCT processed considerable information to quantify the impact (financial/reputation/welfare/legal etc) and focused on corporate work-arounds under the close scrutiny of the EMT.

3.4.2 In the main, Service Level Business Continuity Plans were not activated until after the corporate plan was invoked and in some areas once activated the plans were inadequate. However, there were significant amounts of good practice executed by managers during the incident. Again there is evidence that the Business Continuity culture can be broadened and deepened across the organisation, which is rightly recognised within the Corporate Risk Register.

3.4.3 At this stage there is no ICT Disaster Recovery Plan. This is already recognised as an area of significant weakness and is being given a high priority in the ICT service response.

3.4.4 Following the critical stage of the incident a recovery strategy was developed and communicated to all Heads of Service for implementation in their business areas

3.5 Security

3.5.1 The importance of ICT Security was firmly considered in all decision-making and was not compromised.

3.6 Personnel Welfare

3.6.1 Welfare of all staff was considered at all stages and feedback mechanisms set up and proactively acted upon. Although there were challenges in all areas particularly in areas with customer facing staff, all services managed to deliver their services with minimal impact.

4.0 Financial Impact

4.1 The post incident review considered the financial costs arising directly from the ICT incident.

4.2 As part of the exercise Heads of Service were asked to maintain records of financial costs incurred, including direct costs associated with

- staffing (for example recruitment of agency staff to cover a backlog of work)
- loss of income (income not collected rather than delayed)
- third party costs

4.3 It is recognised that there was significant disruption and loss of productivity however it is not possible to quantify this in direct financial terms.

4.4 The costs incurred directly by ICT total £1.2m. These include £600k for the provision of consultancy support and expertise to resolve the ICT issues plus an additional £600k for the purchase of additional Wyse terminals to replace PCs as part of the recovery strategy. The Wyse terminals costs would have been incurred anyway, the spending was brought forward because of the virus.

4.5 The direct costs incurred within services totalled £247k. The main elements of this include:

- £178k staffing costs with £169k covering the processing backlog for benefits and for council tax and £5k in for overtime costs in Payroll and the Shared Service Centre.
- £45k lost income which mainly relates to bus lane enforcement notices which had to be voided
- £23.5k other costs including additional third party support and compensation payments due to the delays in the processing of benefits claims.

5.0 Lessons Learnt

5.1 EMT membership to be established clearly at the outset of any incident and remain flexible throughout in order to response to the various challenges.

5.2 Embed pertinent lessons and review Corporate Business Continuity Plan by August 2009.

5.3 Further embed the Business Continuity culture across the organisation through awareness raising and training/exercising of Business Continuity processes and crisis management procedures with senior managers.

5.4 Commence enhancing the resilience of support services that are corporate dependencies to service business continuity plans such as ICT, Personnel and Property.

5.5 Internal crisis communication procedures need to be made robust and build on recent achievements.

5.6 Ensure communications with regulatory bodies are included in all external communication strategies i.e. Information Commissioner, external auditors etc.

5.7 Better processing of significant Council wide impact information needs to be considered and put in place.

5.8 Develop an ICT Disaster Recovery Plan.