

<b>Committee(s)</b>	<b>Dated:</b>
Digital Services Sub-Committee – For Information	26th September 2019
<b>Subject:</b> IT Division – IT Service Delivery Summary	<b>Public</b>
<b>Report of:</b> The Chamberlain	<b>For Information</b>
<b>Report author:</b> Eugene O’Driscoll, Agilisys Service Director Matt Gosden – Deputy IT Director	

### Summary

There was a total of 4 P1 and 6 P2 incidents for the City of London Corporation and City of London Police in July. 7 of these incidents were caused by external factors such as supplier works outside of the direct control of the IT service.

With respect to the IaaS outage on the 4<sup>th</sup> of July at 08:28 multiple alerts were observed as the IBM primary production storage device suffered an unexpected malfunction, triggered by planned power maintenance work by datacentre owners COLT to Agilisys storage equipment which caused damage and required hardware replacement. This affected access to network drives, ArcGIS and Mosaic, amongst others. Agilisys takes full responsibility for its supplier and recognising the significant impact of this failure and has volunteered compensation to City of London which was accepted by the Deputy Chamberlain.

Problem records have been created where appropriate to identify root causes and to manage improvements.

- There were **3** P1 incidents for City of London Corporation and **1** for City of London Police.
- There were **2** P2 incidents for the City of London Corporation and **4** for City of London Police.
- The Net Promoter Score average for the City of London Corporation/City of London Police for the last 3 months is **+77**. Any score over 50 is considered very good.
- **92.5%** of users reported a good or very good experience of the City of London Service Desk.
- **100%** of users reported a good or very good experience of the City of London Police Service Desk.

### **Recommendations**

*Members are asked to note this report*

## Main Report

### Service levels and exceptions

#### 1. City of London Police (CoLP)

##### P1 incidents

There was 1 P1 incident

Affected Service	Reason	Resolution	Problem Management plan
Internet browsing	Vodafone patching of their central firewalls causing ICMP packets to be denied	The change was reverted by Vodafone	Supplier management

##### P2 Incidents

There were 4 P2 incidents

Affected Service	Reason	Resolution	Problem Management plan
External outgoing email	Vodafone renewed a TLS certificate causing external outgoing email delay for up to 2 hours for a subset of users	Vodafone (Fujitsu) reverted the certificate change	Supplier management
IMS/DRS CCTV	Users were unable to login using normal login credentials	Resolved by 3rd party BT	In project mode
Niche	Niche was running slowly, and the database was locking due to high CPU usage	Resolved by 3 <sup>rd</sup> party Lincs Police	Supplier management
HR Origin self service	Users were unable to login to the HR system	Resolved by 3 <sup>rd</sup> party Capita	Supplier management

#### 2. City of London (CoL)

##### P1 incidents

There were 3 P1 incidents

Affected Service	Reason	Resolution	Problem Management plan
Telephony and data services	A failed change to upgrade infrastructure impacted	The infrastructure change was reversed.	The change was reviewed, and the

Affected Service	Reason	Resolution	Problem Management plan
	services in HARC, Contact Centre and other locations.		root cause of the failure understood.
Guildhall Events WiFi	Temporary power failure caused the Guildhall Events WiFi to be unavailable.	O2 did not make any remedial changes and advise that local power issues were the cause.	Escalated to CoL IT for review.
IaaS, affecting multiple services	A failed change to upgrade infrastructure affected multiple services for 1 day.	The change was reversed, and damaged hardware was replaced.	Agilisys carried out a full review of its supplier processes.

## P2 Incidents

There were 2 x P2 incidents

Affected Service	Reason	Resolution	Problem Management plan
IDox	Monthly security patching of the IDOX servers caused an issue for IDOX public service module.	The server was re-patched and restarted.	Improved testing following monthly patching.
Pubnet	The VPN that supports the connection to Pubnet failed.	The supplier restarted the VPN.	Escalated to CoL IT for review.

Service performance summary is detailed in the dashboard below.

## Gauges to monitor performance – July 2019



## **Service improvements**

### **3. Police Improvements include:**

- Improvements have been made to the monitoring and alerting of CoLP systems, including refinements to assist in more realistic and real-time alerting for server capacity.
- Work is ongoing to review and refine critical applications and systems at CoLP and improving the 3<sup>rd</sup> party support to align with the business requirements.
- Following initial feedback from the 2019 IT health check, prior to the publication of the full report, work has been carried out to remediate findings to improve security in some key areas.

### **4. Corporation improvements include:**

- Following the IaaS (infrastructure) outage on the 4<sup>th</sup> July Agilisys will work, free of charge, with the Corporation to mirror agreed key applications across the IaaS infrastructure. This will provide higher levels of resilience and more protection against infrastructure and connectivity issues in the unlikely event of a similar incident.
- Agilisys signed an agreement to manage the network supplier Roc on behalf of the Corporation. This will ensure that there is a single point of contact for IT issues and that this correctly sits within Agilisys end-to-end principles of supplier management.
- RedSixty (contractor) continue to conduct local site surveys of all existing Communications and data rooms, including UPS devices in order to establish an “as is” awareness of electrical resilience throughout the estate. Once completed these surveys will allow CoL to make an informed decision regarding an ongoing management and maintenance schedule for all Uninterruptable Power Supply devices based on a tiered communications room classification, where a Tier 1 room would contain critical equipment for example and would therefore require improved power resilience and security.
- In Parallel, the City Surveyors Team are carrying out an audit of the air conditioning and environmental services in all Guildhall Comms rooms to identify and remediate any discovered issues.
- A full vulnerability scan (like the scan performed as part of PSN) has been completed across the CoL network and all servers to ensure that the estate is as secure as possible. This will be repeated every 3 months to provide additional security assurance.
- Work continues to develop a Public/Guest Wifi solution for the CoL/CoLP estate. A High-Level Design (HLD) has been created and is currently under review.

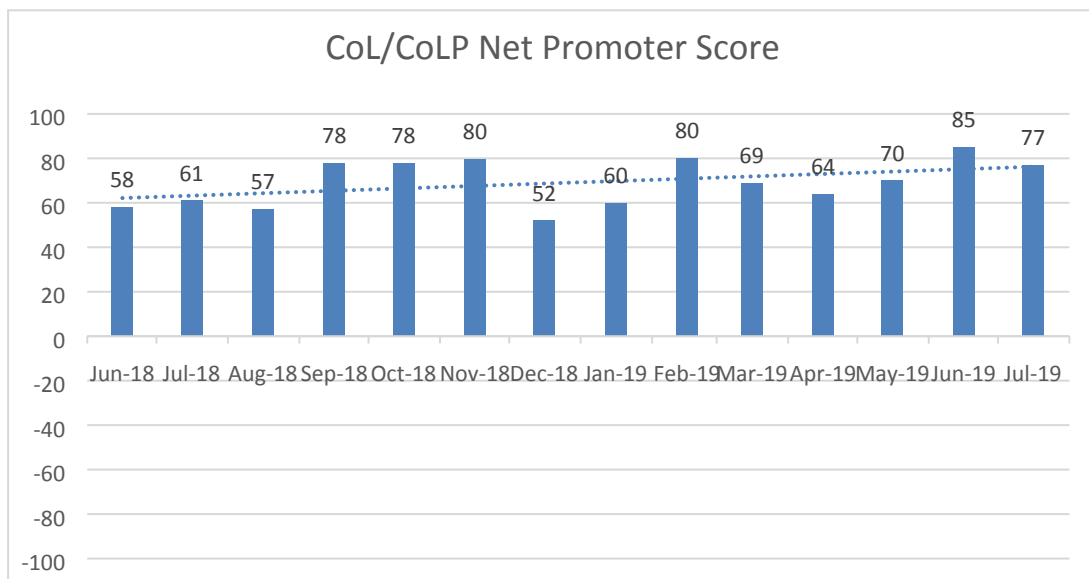
## 5. NPS (Net Promoter Score)

- NPS has been running for over a year at City of London and City of London Police to return a joint rating based on a single question “Based on your experience, how much would you recommend the IT service to your colleagues?”
- Customer’s rate between 0 and 10, where 0 to 6 is considered a detractor, 7 and 8 are passive scores and 9 or 10 are promoters.



$$\text{NPS} = \% \text{ 😊 } - \% \text{ 😞 }$$

- The percentage of detractors is subtracted from the percentage of promoters to give a possible score in the range -100 to +100.
- Results are displayed in the graph below and have consistently shown what is a very good score, often well above +50. Additionally, a gradual overall improvement is shown by the trend line since last June 2018.



## 6. Disaster Recovery Testing

- As outlined previously to Members, on the 26<sup>th</sup> June we performed our annual Disaster Recovery (DR) test which revealed a priority issue where the secondary connection to the BT provided Wide Area Network did not failover as expected. It was later discovered that the network routes were not configured correctly by BT for this to work.
- Following some technical changes, on the 13<sup>th</sup> August 2019 we conducted a follow up DR Test for this service. Testing revealed that only half of the

remote sites would continue to connect to the Guildhall in the event of a major network outage.

- Our networking partners are developing a solution to resolve the issues the testing revealed. We expect to have implemented the solution by the end of September 2019.
- One of the other key findings from the DR test was the proximity of key BT equipment, meaning that the loss of this specific data room could pose a significant risk to external connectivity for CoL. The solution to this is also being developed with our networking partners.
- As requested by Members, a broad-scope DR test is being developed for our website and supporting architecture. These tests will include:
  - Loss of a datacentre or services within it;
  - Loss or inability to access of data hosted on a key website server;
  - A simulated Distributed Denial of Service (DDoS) and/or ransomware attack.
- The results of the test will be communicated to Members and any lessons learned will be assessed when CoL review the interim website stability and security options being presented to CoL by Agilisys and being developed in parallel.

**Matt Gosden**  
**Deputy IT Director**  
**T: 07714 746996**  
**E: [Matt.Gosden@cityoflondon.gov.uk](mailto:Matt.Gosden@cityoflondon.gov.uk)**

**Eugene O'Driscoll**  
**Client Director – Agilisys**  
**T: 07557 150020**  
**E: [Eugene.O'Driscoll@cityoflondon.gov.uk](mailto:Eugene.O'Driscoll@cityoflondon.gov.uk)**