Dear Joint Committee member,

Please see below the briefing note on the global IT outage of Friday, 19 July 2024, caused by a CrowdStrike update.

Brent, Lewisham and Southwark are CrowdStrike customers. We have 934 Windows servers, of which 932 had the CrowdStrike agent installed. The servers received a routine update of the CrowdStrike client at approximately 5:30 on the morning of July 19, 2024. When the update was received, a logic error in the code, caused the servers to crash and the servers would not recover without manual intervention or restoration from backups.

At that point, when all servers crashed, essentially all councils' services were down for all, as authentication for anyone to log in was not available. Staff could log in to their laptops using cached credentials, but other services like Outlook, Teams, and front-line applications were offline. There may have been a few applications hosted by 3rd parties that may have worked, especially if they required a unique login and password, but fundamentally the council could not operate.

Brent and Lewisham's websites were up as they are externally hosted, but not all website services were available. Southwark's website was not operational until approximately 11:00 due to larger dependencies on other services that were offline. It was not until around 14:00 that most of the website features for all council websites were available when other application servers were restored.

The shared service discovered the issue around 6:30 am and put a team together, the team focused on Tier 0 services (Underpinning infrastructure, network connectivity, authentication etc), we spoke with CrowdStrike and received the information needed to recover the services, this took us until approximately 10:30 for Tier 0, from around 10:00 we started to recover Tier 1 applications (Social Care systems, Housing, ERP, Revs and Bens, etc) this took us until around 14:00, we were meeting with the councils every hour on the hour for the prioritisation of the recovery of services, we then focused on Tier 2 and 3 services (libraries, street cleaning, planning systems etc) which continued until around 18:30, almost all services had been restored but some additional servers were needed over this weekend and some more work although minor was still needed on Monday morning.

Our recovery methods were a mixture of what CrowdStrike provided, and in some cases where data integrity was not an issue, it was quicker to recover from a backup taken approximately 21 minutes before the crash, we were incredibly lucky with the timings of this incident as we had very recent backups also we had the CrowdStrike agent installed on laptops for council members and senior managers as additional assurance over the recent election period, the fact that most laptop users would have been offline when the software update was released meant that they didn't receive the update and we avoided a much larger issue.

In summary, council core services were unavailable from around 05:30 until around 10:00, when they started to recover until 14:00, and less critical services recovered between 14:00 and 18:30 and some bled over the weekend and Monday morning; if you have any specific questions about this incident, please feel free to reach out to me.

Fabio Negro
Shared Technology Services