Post-incident analysis report – March 2015

Brief description	UCAS Data for HESA Transaction (Star J files) – incorrect data	Web-link – loss of features	UCAS firewall – DDOS attack	Web-link – unable to process applications
Date	23 February – 5 March	12 March	25 March	26 March
Details of problem experienced	On the 23 February several providers identified an incorrect UKPRN for some of their applicants in the *J file. This resulted in incorrect HESA returns and reporting for those providers who use this data in their MIS systems.	At approximately 11:50 the virtualised windows platform suffered an outage. This prevented providers from adding, amending and deleting course or institution details via web-link	At approximately 23:15 our firewall provider suffered a DDOS attack on one of their upstream providers. This caused several UCAS services to become unavailable including, UCAS.com, link services, Track and Apply. This affected overnight batch jobs for providers and applicants ability to manage their application during this period.	At approximately 12:10 it was identified that providers could not process applications. An error message was returned when providers attempted to set decisions on web-link.
Resolution	The data was corrected and re-presented to the affected providers on Thursday 5 March.	As part of a planned security upgrade across our virtualised windows platform a server re-boot was required however, this was performed incorrectly causing an outage. This was resolved with a sequential reboot of the data core servers on which the virtual windows platform runs on. At approximately 15:30 full service was restored.	At approximately 00:11 our provider re-routed traffic to their London Datacentre restoring service.	The web-link application ran out of available connections to the database. The application was restarted to free up the connections already in use, most of which were dormant. Normal service was restored at approximately 13:20.
Actions taken to prevent a repeat incident	We have undertaken an extensive exercise to better align the mapping of the data in the reference table which holds the UKPRN and is used to output this data in the *J. This will help mitigate any issues around the UKPRN for future *J files.	The configuration management database that stores the dependencies between services has been updated to ensure this incident is not repeated.	In partnership with our firewall provider additional infrastructure has been implemented increasing redundancy and failover capability.	The connection pool size along with the way the application handles existing code is under review as part of our Confirmation and Clearing preparations. Any changes will be tested with loads in excess of predicted peaks.

We appreciate that some of these incidents will have caused you some inconvenience and would like to assure you the resolutions were implemented in such a way as to maintain applicant data integrity. Full assessments were also carried out to ensure there was no impact on the data integrity for those providers affected.

If you have any questions or concerns please contact your dedicated Technical Relationship Manager.

Kalvyn Griffiths – London and South East
Adam Glaudot – Northern England, Scotland and Northern Ireland
Tom Gromski – East, Midlands, South West and Wales