FUJITSU

Mission Critical Australian Government Health Technology

This Australian government health agency provides Information and Communication Technology (ICT) business systems and services to the state public health sector. They ensure that the infrastructure, applications and data flows needed to operate 200 public hospitals and over 80 community health services are operating 24/7 so that the healthcare workforce can get on with the business of patient care.

Fujitsu provides the managed service that keeps systems stable, functional and able to cope with on demand fluctuations from the public health services.

Challenge

As part of a routine Operating System upgrade, patches were scheduled to be applied to upgrade cybersecurity and bring the system up to specification. In order to make sure that the patches would work, the team had to run a test script to check disk status. The test detected disk errors.

As a result, activity needed to be paused until the vendor could vacate the disk drive and arrange a replacement, however, the system remained vulnerable to the issues known to be addressable through the patches. This issue eventually aggravated the system performance and caused disruption for the end users.

Instability was experienced across many applications, which resulted in the workforce at multiple public hospitals unable to operate some applications. Some Hospitals had to work in Code Yellow resorting to pen and paper as a means of business continuity.

Solution

A technical **war room was created**.

The team worked 24/7 and brought in additional technical specialists to minimise downtime.

Fujitsu initiated its **Major Incident Remediation Methodology**.

The incident was immediately raised and a Major Incident instigated as multiple Hospitals were impacted by performance issues. A technical war room was created across both Fujitsu onshore and Global Delivery Centre teams as well as the vendor onshore and offshore and customer teams onshore. The team worked 24/7 and brought in additional technical specialists to minimise downtime.

Fujitsu initiated its Major Incident Remediation Methodology including investigations, technical health checks, change reviews and trouble-shooting as part of a multi-pronged assault to achieve problem resolution. Working closely with the customer Applications team, Fujitsu performed health checks across all the Servers (Windows/Citrix/AIX), Storage SAN/Backups and the Networks (LAN/WAN) across both Data Centres to investigate what was causing the performance issues.

The initial approach was unable to identify the cause, let alone the solution but the multi-vendor team persisted. As part of the process of elimination, the vendor's investigators based in the lab environment completing technical reviews suggested rebooting the Hosts to re-instate the storage connections to the servers.

Fujitsu received approval from the customer to proceed with the reboot and shortly after, the reboots fixed the performance issues. The Hospitals confirmed everything was back to normal and the Code Yellow was called off.

Outcomes

The strong multi-vendor collaboration and clear customer communications enabled the incident to be quickly identified, assessed and resolved. Fujitsu, the vendor and the customer worked together as one team to restore the services promptly resulting in a sharp reduction in the time it might otherwise have taken to restore health services at the affected hospitals.

Both the vendor and the customer were able to introduce Service Improvements to prevent the incident recurring. The customer was pleased with the way that Fujitsu's mission critical approach had led to a good outcome for healthcare workers and their patients.

Fujitsu's mission critical approach led to a good outcome for healthcare workers.

www. fujitsu.com/au info@au.fujitsu.com +61 2 9776 4555

FUJITSU