GoAhead

Databarracks' case study

LEADING PUBLIC TRANSPORT OPERATOR USES BACKUP AS A SERVICE TO RECOVER FROM RANSOMWARE

About Go-Ahead Group

Go-Ahead is a leading public transport operator connecting communities through bus and rail services. They operate the UK's largest public transport proof of concept programme. To date they have won 10 international contracts across five countries. They currently operate rail services in Norway as well as bus contracts in Australia, Singapore, Sweden and Ireland.

Databarracks

The Challenge

Databarracks has provided Backup as a Service to Go-Ahead Group for all sites including two data centres since 2016.

On September 6th 2022, Go-Ahead Group experienced a ransomware attack.

Alan Harvey, Head of IT Operations at Go-Ahead Group:

"Our organisation provides important transport services in several countries, and we're the biggest bus transport provider in the UK. So, cybersecurity and Business Continuity planning have always been top priorities. We have robust security measures in place, but it's impossible to protect against every eventuality. Organisations will inevitably face a successful breach at some point.

"In early September 2022, we found ourselves facing precisely this scenario. Members of our team who tried to access data found it to be encrypted. They received an error message telling them the organisation needed to pay a ransom in order to decrypt the files.

"It was clear that the attack was designed to maximise impact and speed with encryption operating at the VM rather than file level. This affected entire sections of our administrative operations, though the impact was limited to our back-office systems, rather than on the customer-facing side."

The Solution

"Thankfully, we have air-gapped backups which were unaffected by the attack. Databarracks built and managed them for us, and this is how we recovered from the incident.

"As soon as we realised our system had been infected by ransomware, Databarracks worked with us to establish priorities for the recovery. We had lost our on-premises infrastructure. Our clean backups were in Azure and recovering into Azure was the best option in this incident. Databarracks quickly spun-up dedicated recovery infrastructure for us to accelerate the process.

"Throughout the recovery, the team were constantly monitoring and working to optimise bringing systems back online as quickly as possible. They worked with us to test, validate, tick-off the list, and keep moving through the entire incident.

"Due to the nature of our work, we needed the fastest response and recovery times possible. Databarracks tailored a communications system for our case so they could communicate directly with our Crisis Response Team members. Clear communication during a crisis is critical and there were a lot of things we needed to get over the line very quickly, so this was immensely helpful."

The Benefits

"One of the major benefits of working with Databarracks is that they have specialists with in-depth knowledge and experience of the infrastructure and applications we use. When we were hit by this cyber-attack, that meant we could rely on them to action our highest priorities immediately.

"In the aftermath of the attack, we carried out a detailed post-incident review to assess areas for improvement. In addition to changes in preventative security, Databarracks were able to help us drive changes in segregation and configuration to help improve the speed of response and recovery.

"Throughout the recovery, the team were constantly monitoring and working to optimise bringing systems back online as quickly as possible"

"For us, that means we have reassurance that this kind of incident is less likely to happen again. And if it does, the recovery process will likely be much simpler.

"Finally, throughout the incident, Databarracks not only recovered our systems, they were also always on hand to advise us. In a crisis, having a dedicated team of specialists to problem-solve for the most urgent issues was vital.

"From when we first encountered the breach, Databarracks was working to recover our systems 24/7. From building new infrastructure to recover our data, to advising on how we can further bolster our security in the future as the threat landscape continues to evolve.

"It is widely accepted now that it is no longer possible to guarantee the prevention of a cyber incident. It is inevitable that at some point, organisations will face a successful attack. The measure of success now is how quickly we can detect, respond, recover, and limit the impact on business operations. Databarracks was key to helping us do exactly that."

0800 033 6633
contact@databarracks.com
www.databarracks.com

Databarracks,
1 Bridges Court,
London, SW11 3BB

Databarracks

About Databarracks

Databarracks is the UK's specialist business continuity and IT disaster recovery provider.

In 2003, we launched one of the world's first true managed backup services to bring indestructible resilience to mission critical data.

Today, we deliver award winning data and continuity services supported 24/7/365 by our team of handpicked experts.

We make enterprise-class continuity, security and resilience accessible for organisations of all sizes.

0800 033 6633
contact@databarracks.com
www.databarracks.com