



BCDR Case Study

Business Services | Business continuity and disaster recovery (BCDR) solution | UK National

01. summary

Our client is a well-established service business with 30 branches and 180+ staff across the UK. Like many businesses in the service sector, they rely on various essential systems and applications.

With an in-house IT team of 3, who managed their day-to-day IT needs, they came to Nexus looking for a business continuity and disaster recovery (BCDR) solution to ensure their data was fully backed up and recoverable should the worst ever happen. They invested in our comprehensive Nexus Cloud Connect (NCC) BCDR solution which offers:

- Complete backups taken every 5 minutes
- Insider Threat Protection
- Optional Continuous data protection
- Infinite retention of cloud backups
- Complete automated end-to-end solution
- No tapes or disks to take offsite
- All back-ups tested and verified
- Server recovery in under 45 seconds
- DR Rehearsal

The client recognised the importance of disaster recovery and robust backups, so they took this solution out for peace of mind but initially saw it as a type of insurance policy they'd probably never have to use.

02. challenge

Some months later we received a call on a Monday morning from our client to say that their whole system; servers, platform, VMware, applications - everything had been deleted.

Their team had lost access to all their systems. When the in-house IT team went to check on the offsite and on-site backups; they had also disappeared. Panic had set in.

It was discovered that a hacker infiltrated their systems via an unpatched Microsoft Exchange vulnerability one week earlier and had been harvesting local IT administrator credentials, later encrypting everything they could find.

Unfortunately, their Exchange had not been properly patched which left it vulnerable to attack.

Needing to process £1m worth of payroll, pay suppliers and invoice their clients, they required their systems back up and running as quickly as possible.



03. solution

Our team immediately sprang into action to recover everything this client had lost and get their operations back up and running as swiftly as possible.

Part of the NCC solution includes Insider Threat Protection, which means that you have an additional backup of your systems behind a secure firewall that is invisible to hackers. The hacker had not been able to locate this protected backup and having assumed all was deleted, thought the job had been done.

After carrying out thorough tests, scanning for possible malware and ensuring the environment was safe to enter, we carefully started reconnecting the team back into their system. Thankfully we were able to spin up all of this client's data, systems and applications within a matter of minutes, hosting them in our dedicated disaster recovery centre.

The client had access to this secure environment for free for 30 days whilst their own on-site and off-site servers were restricted and assessed.

04. testimonials



The client's IT Manager comments

"We took this solution out as it felt like the perfect backup option should the worse ever happen, but we genuinely never thought we would actually need to use it. Unfortunately for us, we did need it and it performed even better than expected. As soon as we made the call, the team jumped into action and got us safely up and running with ease and in a timeframe that meant our business operations didn't suffer.

It's hard to think about where our business would be now if we didn't have the Nexus NCC solution in place. We never saw this attack coming and like everyone, you always think these things will never happen to you, but we're living proof that they do and when it does happen, you want reassurance that your business will survive. This solution offers that."

Security Specialist Julian Dean adds

"We developed this system because we understand the pain businesses experience when they suffer a breach. It can ruin reputations, impact staff morale and ultimately in some cases, bring businesses to their knees. With the Nexus NCC solution in place, we offer clients a more positive outcome. Their systems are safe, and downtime is massively reduced, from what can be days, or even weeks to a matter of just minutes.

It's a solution we recommend to every client, no matter their size or industry. We've had to implement it on numerous occasions now and each time, the unfortunate client has felt it was the best investment they'd made."



The Nexus logo is positioned in the center of a large, solid orange rectangle. The word "nexus" is written in a lowercase, sans-serif font. The letter "x" is stylized with a diagonal line and two small circles, one on each end, giving it a molecular or network-like appearance.

nexus