DATA MANAGEMENT & INFRASTRUCTURE 365

CASE STUDY

A Rapid Recovery from Ransomware

When a leading international automotive business suffered a ransomware attack, Covenco was able to recover the clients data, giving them initial business continuity within 48 hours.

Customer:
A leading automotive distribution and property business based in the UK.

Industry:
Automotive development, distribution and certification.

Operations:
International presence in the UK, Ireland, Sweden, Finland, Denmark, China and the Baltic states.

IT operations with a data centre based in the Midlands, UK.

Covenco Solutions:

- Disaster Recovery Plan
- Backup as a Service
- Forensic Recovery Services
- Ransomware Recovery Service
- Threat Hunting Service
- Tape-Out Service

Covenco's ship to site equipment includes servers, storage and networking - all ready to be deployed within hours anywhere in the UK.

Background

This customer is a leading UK-based automotive and property business, with over 500 staff across business and operations centres worldwide.

Covenco has supported this customer with various data protection and infrastructure solutions for over 15 years.

Initially providing business-critical ERP hardware and infrastructure solutions based around IBM Power Systems with High Availability, Covenco went on to provide Cloud Backup, Replication, offline backups and complete disaster recovery services.

On 8th October 2022, Covenco received a call from the customer at 1:20 am invoking their Disaster Recovery plan in response to a Cyberattack on their business. The Covenco incident team immediately responded rapidly to determine whether their offsite backups and replica servers were affected and to begin a recovery process.

The Challenge

The customer had received a call from the National Crime Agency (NCA) just two days before the Ransomware attack was executed.

The NCA informed the customer that their organization's name had been highlighted in another ongoing investigation, and they had intelligence to suggest that their internal network might be compromised.

Additionally, the NCA believed the customers' data had been exposed on the dark web. The customer assumed that this was a malicious call and ignored it. Subsequently, after discussing this with the Police, they confirmed that it was a bonified call.

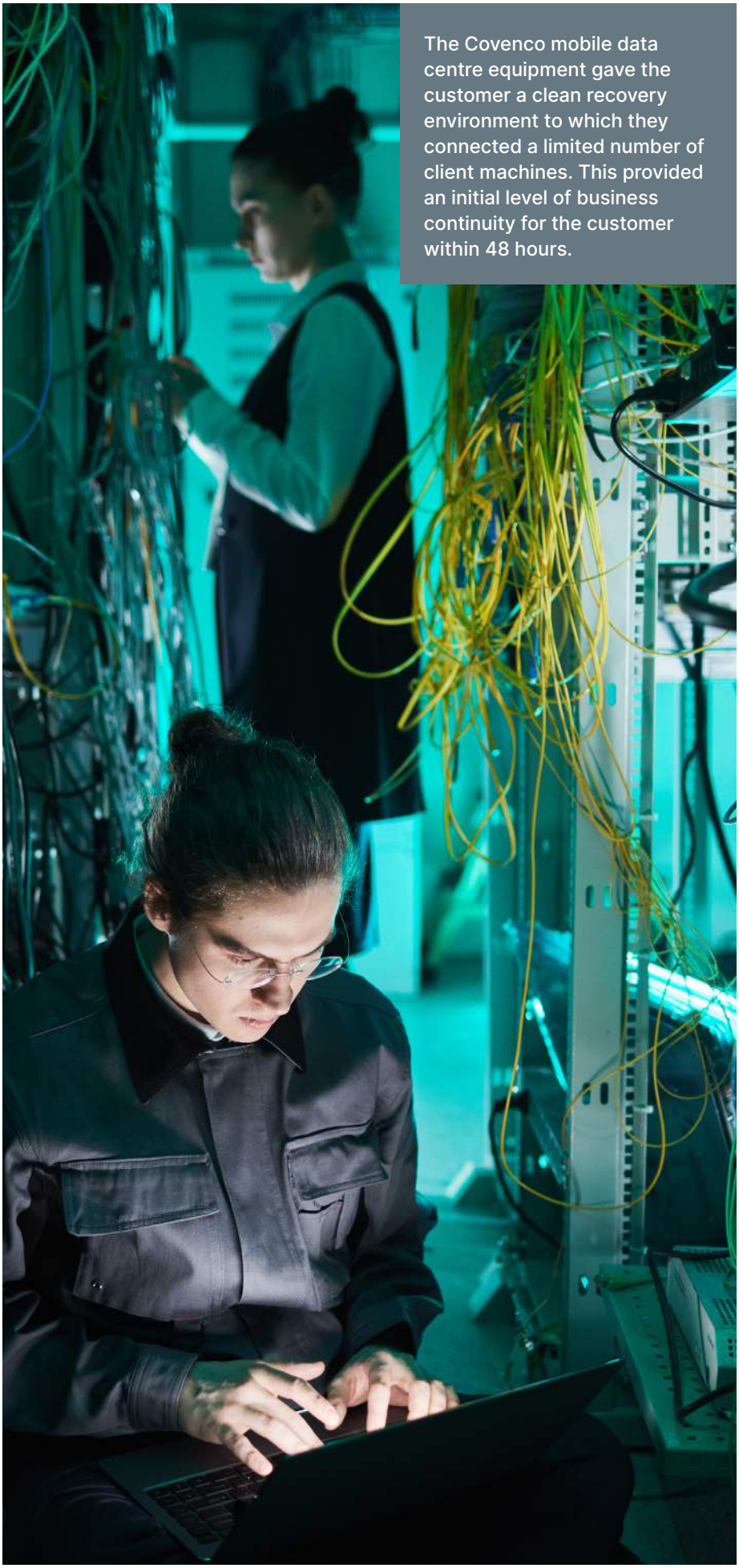
The customer's internal IT team was placed on red alert, and they checked for any abnormal behaviour but found nothing to suggest they had been attacked.

Unfortunately, just days later, it became evident that they were under attack and were the victims of a highly sophisticated Ransomware attack by the Bian Lian Ransomware Group.

"If you receive a call from the National Crime Agency (or other law enforcement) reporting that they witnessed activity on the dark web linked to your organisation, you have to assume that your network has been compromised. The NCA will only call if they have seen activity relating to your organisation and they will not provide any detail, due to risk of compromise to an ongoing NCA investigation".

Gurdip Sohal
Director, Covenco Ltd.

Covenco's immediate advice was to remove all systems from the internet, disable the network and isolate as much of the infrastructure as possible, including all servers, storage, and network appliances.



The Covenco mobile data centre equipment gave the customer a clean recovery environment to which they connected a limited number of client machines. This provided an initial level of business continuity for the customer within 48 hours.

By the time the network was isolated, the Cyber attackers had traversed across all areas of the network, encrypting their local virtual servers and deleting local and partially offsite backups. The next step included a review to see if the offsite online backups held at Covenco had been affected.

Approximately 4TB of the 13TB Cloud Backup Repository had been deleted, but all Virtual server replicas were intact and available for recovery.

The Initial Recovery

Because the Client's existing hardware had been infected, it was crucial to understand how the attackers penetrated the network and how far they had travelled. Covenco, supported by their Incident Response Partners, carried out a full Compromise Assessment to determine a timeline of events and help identify the initial point of access.

The customer also engaged their firewall vendor's incident team to help investigate whether their Firewall had any signs of infection or malware. During this time, Covenco also started a data recovery process by powering on the clients' replicated Servers within the Covenco Cloud Recovery platform.

The team had little confidence in the Firewall being free of infection, so Covenco also restored all the customers' virtual machines to a mobile DR inventory consisting of high-performance IBM storage, Fibre Switch Infrastructure and VMware Host Servers, which were relocated and installed in the customers' data room.

The Covenco mobile data centre equipment gave the customer a clean recovery environment to which they connected a limited number of client machines. This provided an initial level of business continuity for the customer within 48 hours.

It was vital to start the full data recovery to clean infrastructure. As part of the invocation process, Covenco restored each server backup to an isolated SAN box environment and ran a security scan against each

Covenco's mobile data centre gave the customer a clean recovery environment, providing an initial level of business continuity within 48 hours.

backup to ensure they were not restoring any Malware or infections.

Once the scans were completed, the backups were placed into production mode, ready for the customers' use.

While the recovery environment was being relocated and installed at the customer site, Covenco initiated a new Veeam backup server so any restored data could be immediately protected. The Covenco team maintained constant contact with the customer throughout the invocation, assisting in data recovery and providing access to remote replicas once they were deemed safe.

Post-incident response and actions.

Once the compromise assessment had been completed, Covenco commenced a Threat Hunt by installing Carbon Black EDR toolsets onto the newly recovered environment, which immediately began learning about the customers' IT environment to identify any anomalies and 'back doors' left behind by the attackers.

The threat hunt was proactive, sending all alerts to a Security Operation Centre (SOC) where highly skilled security experts were on hand to address and remediate any anomalies found.

Ongoing protection

Following guidance from Covenco, the customer introduced fully managed Extended Detection and Response services along with managed SEIM and SOC Services. These solutions were able to gain greater visibility into the customers infrastructure and network, delivering the piece of mind that comes with 24×7 monitoring by highly skilled security professionals.

Additionally, an Incident Response Retainer is now in place to deliver instant access to emergency incident responders and help fight and remediate future cyber attacks.

Are you ready to protect your critical business data?

Contact the Covenco Ransomware Recovery team to discuss your security measures.

We can guide you on the latest best practice tools and techniques to ensure your ransomware survival.

Call: 01753 732000

Email: sales@covenco.com

Visit: covenco.com

About Covenco

With more than 30 years of experience in the IT industry across a range of technologies, Covenco specialises in purchasing, selling and renting new and refurbished IBM, HP, Dell and NetApp computing hardware, storage and supporting software. Today, Covenco provides cloud and hosting solutions, disaster recovery, maintenance, virtualization, backup and high-availability services.

Solution and services used

Covenco Ransomware Recovery Service

Veeam Cloud Connect

Covenco Tape Out Service

Contact Covenco

Covenco
Unit 3-4, MXL Centre
Lombard Way
Banbury
Oxfordshire
OX16 4TJ
United Kingdom

Telephone: 01753 732000
Email: sales@covenco.com

www.covenco.com

covenco
DATA MANAGEMENT & INFRASTRUCTURE 365