

Case Study

MSP Prime ICT Defeats Christmas Eve Ransomware Attack with Arcserve Backup Solution



When ransomware strikes during the holidays, cyber resilience makes the difference between business continuity and catastrophic loss. The Prime ICT Christmas Eve crisis demonstrates how the right data backup strategy protects against sophisticated attacks that can cost organizations hundreds of thousands of dollars.

The Challenge

The Prime ICT monitoring system detected critical server failures at 3am on December 24. The affected customer was on holiday until January 5, unaware their business faced a catastrophic threat. The Prime ICT 24x7 service commitment, supported by monitoring capabilities in the Arcserve ShadowProtect data backup and recovery platform, enabled immediate customer notification and response initiation.

Remote investigation revealed complete network connectivity loss across production servers. The Prime ICT team initially suspected system bugs or failed updates. A readme.txt file on the desktop revealed the true scope: ransomware had encrypted five production servers with a £200,000 Bitcoin ransom demand.

Country: United Kingdom

Industry: Managed Service Provider

Solution: Arcserve ShadowProtect and Arcserve ImageManager with Wasabi cloud storage

The Solution

As a managed service provider (MSP), Prime ICT cyber resilience strategy centered on Arcserve ShadowProtect and Arcserve ImageManager, backup and recovery solutions designed for MSPs to host data resilience for multiple customers.

ShadowProtect delivers continuous data protection through block-level incremental backups with advanced deduplication technology that eliminates redundant data blocks across backup sets. ImageManager automates backup consolidation and maintains optimized recovery points across multiple storage locations.

The data backup architecture included:

- Hourly backups from 7am to 7pm to local NAS storage
- Nightly replication to Wasabi cloud storage
- Comprehensive data protection across production servers

When ransomware compromised local NAS backups, the team pivoted to cloud recovery. At 3pm on December 24, Prime ICT began downloading approximately 6TB of critical business data from the cloud. The customer's 1GB leased line provided sufficient bandwidth, though the data volume required 27 hours for download to complete.

The bare-metal recovery functionality in ShadowProtect enabled a complete system reconstruction from stored images.

The centralized interface of ImageManager provided rapid identification of specific recovery points needed for both full system and granular file-level restoration. The Prime ICT team worked through Christmas Day, monitoring the download and preparing restoration procedures.

Data download completed at 10pm on December 25, with data successfully retrieved, the Prime ICT team-initiated server recovery using the Arcserve WinPE Recovery Tool. The methodical restoration continued overnight, with five servers returned to full operational status by midday on December 26—achieving zero data loss and complete functionality. Forensic analysis revealed this wasn't the customer's first ransomware exposure. Prime ICT identified and removed persistent threats from a previous incident that had included unauthorized remote access tools and keylogging software. The current attack exploited a former employee's account that hadn't been properly decommissioned. Prime ICT implemented comprehensive security enhancements including password resets for user accounts and permanent deactivation of the compromised legacy account. This resolved the immediate crisis and eliminated vulnerabilities that would have enabled future compromises.

The Results

The Prime ICT cyber resilience approach delivered measurable outcomes:

- Complete financial protection – The customer avoided the £200,000 ransom payment, maintaining compliance with regulatory guidance that discourages funding criminal enterprises
- Minimal operational disruption – Full business continuity restored within 48 hours -- despite the holiday timing
- Enhanced security posture – Previously undetected vulnerabilities identified and eliminated

Key Statistics

- £200,000 ransom demand defeated
- 5 servers fully recovered from ransomware encryption
- 6TB of critical business data restored
- 48-hour total recovery timeframe
- Zero data loss achieved

"Ransomware attackers striking during the holidays can cripple an MSP client, but with reliable backup and recovery from Arcserve and fast cloud recovery from Wasabi, Prime ICT was able to keep our customer up and running. The customer did not need to pay the £200,000 and was able to recover all of their data," said Jack Hubbleday, Technical Director at Prime ICT.

Because Prime ICT trusted the award-winning MSP-specialized software from Arcserve, ShadowProtect along with ImageManager and Wasabi cloud storage, the customer's data was available for restore to allow business to continue. Arcserve ShadowProtect is a cross-platform data protection and backup software for Windows and Linux servers. It provides fast, reliable backup and recovery, with specialized tools for MSPs (Managed Service Providers), including centralised management and flexible licensing.

Arcserve capabilities enabled Prime ICT to maintain their 24x7 service commitment and respond rapidly to emerging threats without the complexity of managing multiple backup solutions.

Protect MSP Clients from Ransomware

Don't wait for an attack to test your cyber resilience. Discover how backup solutions by Arcserve can protect your critical data and ensure business continuity. Visit arcserve.com to learn more about implementing comprehensive ransomware protection or [sign up for a free 30-day trial](#) of Arcserve products.

About Prime ICT

At Prime ICT, we are a trusted IT Managed Service Provider (MSP) committed to empowering businesses with innovative and reliable technology solutions. Specialising in VoIP services, network management, cybersecurity, and cloud solutions, we deliver tailored IT strategies to drive efficiency and growth. Our expert team combines cutting-edge technology with personalized support to ensure seamless connectivity, robust security, and scalable infrastructure. With a focus on transparency and responsiveness, we partner with businesses to navigate the complexities of the digital landscape, enabling them to thrive with confidence.

About Arcserve

Arcserve, the pioneer in unified data resilience, protects data from ransomware, cyberattacks, and disasters through simple, flexible, and affordable data protection solutions for small and mid-size organizations. Arcserve is trusted by customers, channel partners, and managed service providers around the globe. Arcserve delivers AI-enabled cyber resilience protection and world class customer support, so IT teams can have streamlined, cost-effective data management and recovery with low TCO.

