SysGroup

EBOOK

Why Ransomware Resilience Matters — and How SysGroup's RRaaS Keeps You Operational

A Practical Guide for UK Organisations

Learn more

Table of Contents

Introduction

Ransomware remains one of the most widespread and damaging cyber threats to UK businesses. According to the **UK Government's Cyber Security Breaches Survey 2025,** 43% of UK businesses experienced a cyberattack or data breach in the past year, with ransomware continuing to be the most severe and disruptive threat type.

The average ransom payment in early 2025 was £157,000, and the total cost of ransomware incidents across the UK is estimated at £3.4 billion. For small and mid-sized organisations, the impact extends far beyond financial loss. Downtime, data loss, and reputational damage often follow, and many never fully recover.

SysGroup's **Ransomware Resilience as a Service (RRaaS)** was created to change that reality by helping organisations prepare for, withstand, and recover from ransomware attacks.

The Ransomware Challenge

Ransomware has evolved from simple data encryption into multi-stage extortion campaigns. Modern attackers often combine encryption with data theft and threaten to leak sensitive information if payment is not made.

They exploit social engineering, stolen credentials, and unpatched vulnerabilities to infiltrate networks. Once inside, they spread laterally, escalate privileges, and deploy encryption payloads across systems.

The **National Cyber Security Centre (NCSC)** continues to identify ransomware as the UK's most significant cyber threat. Research shows that organisations paying ransoms rarely recover fully. Only 32% of those that paid regained complete access to their data. Recovery is often slow and expensive, and 80% of companies that suffer an attack are targeted again within a year.

The SysGroup Solution

SysGroup's **RRaaS** brings together leading technology and experienced consultancy to create a complete resilience service.

It aligns with the **NCSC's guidance** on ransomware preparedness and provides practical, measurable steps to reduce risk and improve recovery outcomes.

Four-Layer Resilience Model

The service operates through SysGroup's **Four-Layer Resilience Model:**

Prepare
Build resilience before an attack

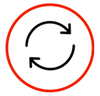
Conduct cyber maturity assessments, incident response reviews, and tabletop exercises to test readiness. SysGroup consultants work with leadership and IT teams to strengthen defences before an attack occurs.

Protect
Stop threats at the source

Implement **Zscaler Secure Edge** to block phishing, malware, and lateral movement.
Deploy **CyberArk Endpoint Privilege Management** to eliminate unnecessary administrator rights and enforce least privilege access across endpoints.

Detect
Identify suspicious activity early

Monitor for privilege misuse and unusual activity using behavioural analytics. SysGroup continuously validates backup integrity and monitors for indicators of compromise across critical systems.



Recover
Ensure business continuity

Use **Rubrik's immutable backup technology** and disaster recovery orchestration to restore data and systems quickly. Recovery plans are validated through test restores and failover exercises to ensure business continuity under pressure.

Shared Responsibility for Ransomware Resilience

Ransomware resilience is a shared responsibility between technology providers and the organisation.

Vendors such as **Zscaler, CyberArk,** and **Rubrik** provide the technical foundation for secure access, privilege control, and data protection. However, each organisation is responsible for integrating these tools into a unified response and recovery plan.

SysGroup's **RRaaS** closes this gap by combining technology management with expert consultancy to deliver complete, measurable resilience.

This partnership ensures proactive preparation, effective protection, early detection, and reliable recovery. By consolidating all layers under one managed service, RRaaS removes complexity and gives you confidence that critical operations can recover from any ransomware incident.

Business Value and Outcomes

SysGroup's RRaaS helps organisations minimise downtime, financial loss, and reputational damage.

Key benefits include:

Faster recovery times, often restoring operations within hours instead of days

Reduced operational disruption and lower total cost of ownership compared to reactive recovery models

Alignment with **NCSC best practice** and international standards such as **ISO 27001**

Simplified management of ransomware resilience through one coordinated service and trusted partner

Conclusion

Ransomware continues to challenge organisations of every size, but with the right resilience strategy, recovery can be achieved. SysGroup's **RRaaS** provides a proven, proactive approach to preventing, containing, and recovering from ransomware attacks. It turns ransomware from an existential threat into a controllable and recoverable event.

Turn ransomware risk into resilience. Learn more at sysgroup.com.