SysGroup

EBOOK

Why Identity Recovery Matters — and How SysGroup's IRaaS Protects Your Business

A Practical Guide for UK Organisations

Learn more

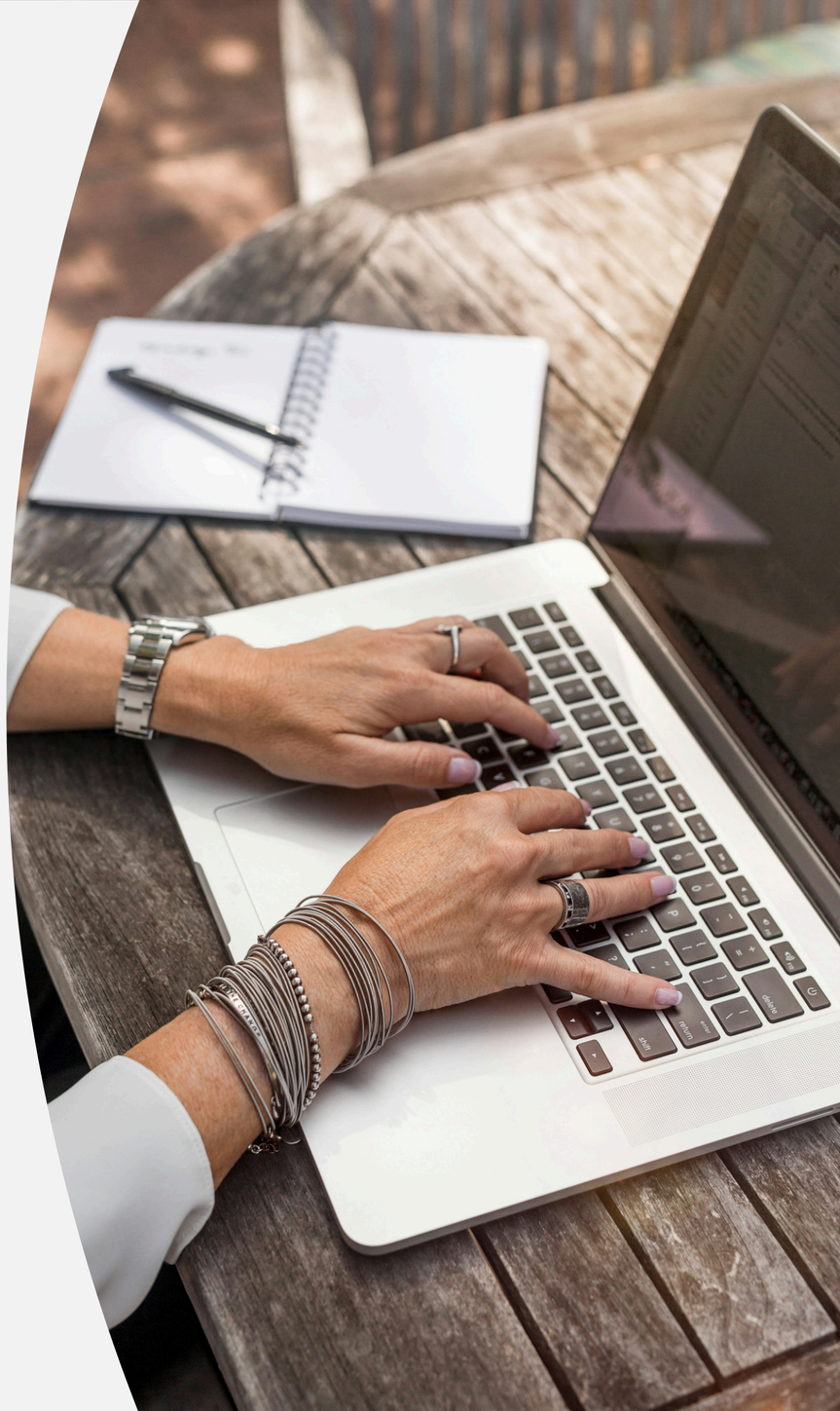


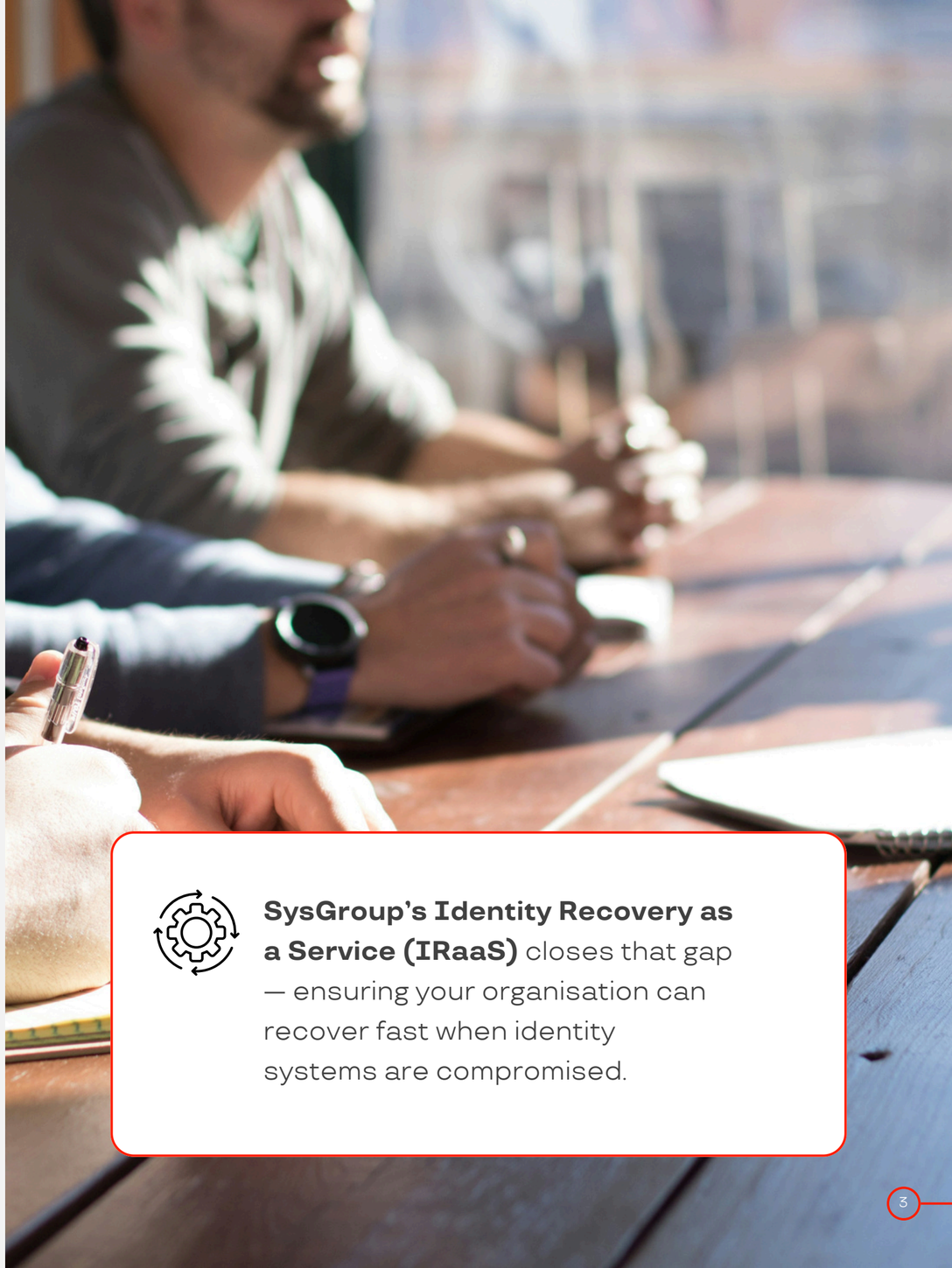
Table of Contents

Introduction

Over
80%

of breaches involve stolen or compromised credentials. Identity compromise can paralyse systems, lock out staff, and expose sensitive data.

While most security efforts focus on detection and prevention, recovery is often overlooked. Without the ability to restore digital identities quickly and securely, even the best defences can't prevent prolonged downtime.



SysGroup's Identity Recovery as a Service (IRaaS) closes that gap — ensuring your organisation can recover fast when identity systems are compromised.

The Identity Threat

An attacker doesn't need to breach your entire network — just one user's identity. Once inside, they can escalate privileges, disable protection tools, and move laterally across systems.

Common causes of identity compromise:

- Weak or reused passwords
- Misconfigured Active Directory or Entra ID settings
- Inadequate privilege control
- Insider threats or human error

The impact:
operational disruption, data theft, compliance violations, and loss of customer trust.

The SysGroup Solution

Identity Recovery as a Service (IRaaS) is a managed offering that helps organisations **recover, restore, and secure** digital identities after compromise.

It's part of the broader **Identity Threat Detection and Response (ITDR)** ecosystem — but focuses on **remediation and recovery,** not just detection.

The IRaaS Framework

SysGroup's IRaaS aligns with **NCSC guidance** and leverages **Rubrik** technology for identity protection and recovery.

Protect

- Immutable backups of Active Directory, Entra ID, and IAM configurations.
- Backups stored securely to prevent tampering after an attack.

Validate

- Regular test restores and attribute-level comparisons.
- FSMO roles, DNS, and trust verification to ensure integrity.

Recover

- Rapid restoration of identity environments after breach.
- Granular object-level rollback for minimal downtime.

Review

- Post-incident analysis and hardening recommendations.
- Updated playbooks to prevent recurrence.

Understanding the Microsoft Entra ID Shared Responsibility Model

Microsoft's Entra ID (formerly Azure Active Directory) operates on a shared responsibility model, where Microsoft secures the cloud infrastructure, but each organisation is responsible for managing and protecting its identity data within the cloud.

Microsoft's Responsibilities:

- Platform security and resilience of the Entra ID service.
- Core authentication mechanisms that enable users to sign in.
- Maintaining availability and operational integrity of the service.

Customer Responsibilities:

- Managing user identities, groups, and access policies within Entra ID.
- Protecting identity data from deletion, cyberattacks, or misconfiguration.
- Managing and securing applications that integrate with Entra ID.
- Configuring Entra ID securely to prevent privilege abuse or data exposure.
- Implementing dedicated backup and recovery solutions to maintain continuity.

While Microsoft guarantees platform uptime, it does not cover identity data loss caused by human error, misconfiguration, or malicious activity. After the default 30-day soft-delete period, restoration of deleted Entra ID objects or configurations can be impossible without a dedicated backup.

Why This Matters

Critical assets

Entra ID controls access to business applications and sensitive data.

Continuity

Dedicated backups ensure quick recovery from deletion or compromise.

Gap in protection

Without your own backup, identity loss can result in operational paralysis.

SysGroup's **Identity Recovery as a Service (IRaaS)** bridges this gap. It provides immutable backups, granular recovery, and proactive validation of Entra ID environments—ensuring your identity infrastructure can be restored swiftly and securely when needed.

Business Value

IRaaS helps your organisation:

Recover digital identities in hours, not days

Prevent re-infection with clean recovery points

Maintain compliance with NCSC and ISO 27001

Reduce risk, downtime, and reputational damage

Delivered as a **managed service,** IRaaS provides end-to-end assurance — from protection through to post-incident review.

Conclusion

When identity is compromised, speed and confidence matter most. SysGroup's IRaaS gives you both — powered by Rubrik, guided by experts, and aligned to national standards.

Protect your identities.

Restore your confidence.

Learn more at
sysgroup.com