SME cyber posture. 2026 baseline.

A regional and sector view of where mid-market cyber controls actually sit heading into 2026, drawn from Numata managed-services data across our EMEA, UK, US and Southern Africa client base.

PUBLISHED	COVERAGE	PREPARED BY	DISTRIBUTION
January 2026	EMEA / UK / US / SA	Numata Business Technology	Public

SUMMARY

Mid-market cyber posture is uneven, and the gaps are predictable.

Across the Numata client base, foundational controls have become widespread, but identity, response readiness and third-party assurance still lag. The pattern is consistent enough by sector and region to plan against.

WHAT WE OBSERVE

01 **Foundations are common, identity is not.**
Endpoint protection and email filtering are near-universal. Conditional Access, phishing-resistant MFA and privileged access controls remain uneven, particularly outside regulated sectors.

02 **Response readiness is thinner than reported.**
Documented incident response plans exist more often than they are exercised. Tabletop cadence and named executive decision rights are the two indicators that separate posture from paperwork.

03 **Third-party exposure is the primary route in.**
Supplier and integration exposure now accounts for a disproportionate share of investigated events. Continuous vendor assurance is still rare in the mid-market.

04 **Regulated sectors set the pace.**
Public sector, financial services and regulated manufacturing consistently show higher control maturity, driven by external assurance obligations rather than in-house appetite.

METHOD

Aggregated, anonymised signals from Numata managed-services delivery, cross-referenced against public incident reporting and regional regulator guidance. Findings describe the client base, not the market as a whole.

LICENCE / ATTRIBUTION