

SME Cyber Resilience 2026–2027

Complimentary strategic briefing • First edition • Europe, Norway and international markets

Executive summary

For smaller and medium-sized businesses, cyber resilience is not simply the purchase of antivirus tools. Supplier dependencies, identity management, backup integrity and recovery capability require board-level decisions. ENISA's September 2026 overview emphasizes ransomware, phishing, exploited weaknesses and risks linked to digital dependencies. This brief is a decision-support framework, not a technical audit of any specific organization.

Three external signals

Published observation	Management implication
ENISA 2026: ransomware remains a high-impact threat	Test the restoration of essential business functions
Verizon 2025 DBIR: third parties involved in 30% of breaches	Map supplier relationships and external access
Verizon 2025 DBIR: vulnerability exploitation rose 34%	Prioritize exposed assets, patching and inventory

Five immediate leadership decisions

- Identity: use multifactor authentication for email, cloud and privileged accounts; review leavers and access monthly.
- Backups: maintain a protected copy and conduct real restoration drills with appropriate recovery-point and recovery-time objectives.
- Exposure: inventory Internet-facing assets, assign owners and set remediation deadlines.
- Suppliers: maintain a dependency register, request relevant control evidence and prepare for service interruptions.
- Response: clarify responsibilities, emergency contacts, basic exercises and draft customer communications.

An actionable executive dashboard

Track MFA coverage for critical accounts; share of assets inventoried; overdue critical patches; successful restoration tests; higher-risk suppliers reviewed; and estimated recovery time in a simulation. Every metric needs a stable definition and a named owner.

Three 90-day decision scenarios

- Scenario A — Defensive baseline: asset inventory, MFA, backups and awareness. Lower operational burden, limited depth.
- Scenario B — Structured resilience: A plus supplier management, recovery tests and quarterly security reviews. Suited to growing SMEs.
- Scenario C — Sector-specific obligations: B plus independent assessment, enhanced risk management and contractual requirements, only when exposure or obligations justify it.

30 / 60 / 90-day action plan

- Days 1–30: define critical services, access paths and dependencies; establish a baseline.
- Days 31–60: deploy prioritized controls and complete a restoration test.
- Days 61–90: run a tabletop incident scenario, review suppliers and report dashboard measures to leadership.

What MSI can offer

MSI can provide non-intrusive maturity reviews, prioritization workshops and governance dashboard design. Technical testing requires written authorization and qualified professionals. No guarantee of compliance, security or elimination of risk is implied.

Sources and limitations

ENISA, Threat Landscape 2026 (22 September 2026): <https://www.enisa.europa.eu/news/exploring-the-evolution-of-the-cyber-threat-landscape-how-dependencies-weaken-our-digital-resilience>

Verizon, 2025 Data Breach Investigations Report: <https://www.verizon.com/about/news/2025-data-breach-investigations-report>

Limitations: public-source synthesis only; no original incident collection, interviews or on-site security audits.