RESILISCORE

FREE INSIGHT REPORT

AI & Emerging Technology Risk Report

Why AI usage is becoming part of cyber resilience for SMEs

Resiliscore | Cyber resilience insight for small and medium-sized organisations

EXECUTIVE SUMMARY

AI is now a cyber resilience issue

Artificial intelligence is moving into everyday business operations through email, office suites, meeting tools, CRMs, e-commerce systems, customer support tools, analytics platforms and public AI assistants. For most SMEs, the main risk is not that they are building complex AI models. The risk is that AI is being adopted faster than governance, security and accountability can keep up.

This report explains the theory behind AI and resilience: why AI usage creates new data, supplier, people, operational and incident response risks, and why those risks should sit alongside traditional cyber controls such as access control, backup, recovery, phishing defence and supplier assurance.

The core message

AI is not separate from cyber resilience. If AI tools touch sensitive information, business decisions, customer communication, software, supplier platforms or employee workflows, they become part of the organisation's resilience picture.

What SMEs often see	What resilience actually requires
AI as a useful productivity tool: faster writing, better summaries, quicker research and automated workflows.	Clear rules on what data can be entered, which tools are approved, who reviews outputs, and how mistakes or data leakage are handled.
AI as a feature inside software they already use.	Supplier visibility: whether AI features are enabled, where data is processed, how outputs are used, and whether staff understand the risk.

The practical SME gap

Recognised guidance now exists for AI risk and AI security, including NIST's AI Risk Management Framework, ISO/IEC 42001 and UK guidance for AI cyber security. The challenge is that most SMEs need the principles translated into plain English, practical governance and manageable first steps.

WHY THIS MATTERS

How AI changes the resilience picture

For SMEs, AI risk usually appears through everyday usage rather than advanced model development. The resilience issue is that AI can quietly affect data handling, supplier exposure, human decision-making, operations and incident response all at once.

1. Data exposure

Staff may paste confidential or sensitive information into public tools or connected copilots.

2. Supplier risk

AI features may be enabled within SaaS products before governance or contracts catch up.

3. Human oversight

Outputs can be wrong, biased or misleading if no review step exists.

4. Operational dependence

Teams may start relying on AI-generated work without checking quality or ownership.

5. Fraud & impersonation

AI increases phishing, deepfake and social engineering risk.

6. Incident readiness

AI-related mistakes need clear reporting, containment and recovery steps.

The issue for most SMEs is unmanaged usage, not sophisticated AI development. Good resilience starts with visibility, control and accountability.

FRAMEWORK LANDSCAPE

What recognised guidance is trying to solve

AI risk is increasingly being addressed through dedicated AI governance and AI security guidance, rather than only through traditional cyber frameworks. For SMEs, the important point is not to become standards experts. It is to understand the direction of travel: AI needs governance, risk ownership, data controls, supplier oversight and secure operation.

Framework / guidance	Plain-English relevance for SMEs
NIST AI Risk Management Framework	A voluntary framework designed to help organisations incorporate trustworthiness considerations into the design, development, use and evaluation of AI products, services and systems.
ISO/IEC 42001:2023	An AI management system standard. It focuses on establishing, implementing, maintaining and improving governance around AI systems, including responsible development and use.
UK AI Cyber Security Code of Practice	UK guidance setting out baseline cyber security principles to help secure AI systems and the organisations that develop and deploy them.
NCSC Secure AI System Development	Guidance for providers and organisations using AI systems, covering secure design, development, deployment, operation and maintenance.

How this links to Resiliscore

Resiliscore does not need to become an AI compliance product. The opportunity is to translate these themes into practical resilience questions that SMEs can understand: visibility, data protection, human accountability, supplier assurance, security impact and incident readiness.

SME EXPOSURE

Where SMEs are most often exposed

Most SME exposure comes from everyday tools and workflows rather than specialist AI systems. The pattern is simple: AI is adopted because it is useful, but resilience controls often arrive later.

Common scenario	What can go wrong
Public AI assistants	Sensitive company, customer or employee data may be entered into external tools without approval.
AI meeting notes and transcriptions	Recordings, summaries or action points may contain confidential material and unclear retention settings.
AI inside CRM, email or marketing platforms	Features may be switched on by default, creating new supplier, privacy and output risks.
Customer-facing content or chat	Incorrect or unreviewed outputs can affect customers, reputation and accountability.
File-connected copilots	Broad access to documents can create confidentiality or oversharing risk if permissions are weak.

The pattern

In most cases, the problem is not the existence of AI. It is the absence of ownership, visibility, boundaries and review.

AI RESILIENCE MODEL

The 6 AI Resilience Questions

These six questions translate emerging AI governance themes into practical resilience language for SMEs.

1

Visibility

Do we know where AI is being used across the organisation?

2

Data protection

What information can be entered into AI tools, and what is off limits?

3

Human accountability

Who reviews important outputs before they are used or shared?

4

Supplier assurance

Have AI vendors, embedded AI features and settings been assessed?

5

Security impact

Does AI increase fraud, access, confidentiality or monitoring risk?

6

Incident readiness

Can we detect, report and recover from an AI-related error or data issue?

This is where AI and resilience meet: simple questions that turn a vague technology trend into practical governance and control.

FIRST STEPS

A practical 30-day starting plan

Most SMEs do not need a complex AI programme to get started. They need a sensible first month of visibility, rules and accountability.

1 Create simple AI usage rules

Set a basic policy for approved tools, acceptable use and sensitive data.

2 Identify tools already in use

Ask teams what AI assistants, note-takers, copilots or embedded features they use today.

3 Set data boundaries

Define what must never be pasted, uploaded or connected without approval.

4 Review supplier terms and settings

Check privacy, retention, model training, permissions and default AI settings.

5 Add human review

Require review for customer-facing, financial, HR, legal or important operational outputs.

6 Update incident response and awareness

Make sure staff know how to report AI-related mistakes, leakage or suspicious activity.

What good looks like in 30 days

- Clearer ownership
- Better visibility
- Safer data handling
- A practical starting point for AI governance

NEXT STEP

How this links back to Resiliscore

Resiliscore does not need to become an AI compliance product to be useful here. Its strength is translating emerging AI themes into practical resilience language that SMEs can understand and act on.

This free insight report is designed to educate and prompt action. The next step is to assess your organisation's wider resilience position and understand where AI sits inside it.

Free assessment

- Complete the free Resiliscore assessment
- Get a high-level view of your resilience position

Full report – £79

- Tailored resilience score
- Ranked priorities
- 90-day action plan
- Evidence checklist and executive-ready summary

Choose the route that suits your organisation's needs.