Report

SMBs in the age of AI: Navigating cyber complexity and building resilience

With research and analysis by

Sage

IDC

Survey methodology and context

Joel Stradling
Senior Research Director,
European Security, IDC

This report draws on findings from a global study conducted by IDC, commissioned by Sage, surveying 2,210 small and medium businesses (SMBs) across eight markets.

The research, published in the IDC InfoBrief SMBs in the Age of AI: Navigating Cyber Complexity and Building Resilience (March 2026; IDC #EUR254487126) and authored by IDC analyst Joel Stradling, evaluates how SMBs are responding to current and emerging cyber security challenges.

It explores their key concerns and security postures in relation to AI and third-party vendor solutions, and identifies the strategic shifts required to move from reactive defence towards proactive security and sustainable, risk-aligned cyber resilience.

The study encompassed the following sectors: financial services, healthcare, telecommunications, energy, manufacturing, resources, retail, software and information services, transportation and travel, business and personal services, education, government, not-for-profit, audit and tax, construction, and hospitality and leisure.

Source: IDC InfoBrief, "SMBs in the Age of AI: Navigating Cyber Complexity and Building Resilience," sponsored by Sage, April 2026, IDC Doc #EUR254487126.

Countries included in the survey

- Canada
- Spain
- United States
- Portugal
- France
- United Kingdom
- Germany
- South Africa

Company size

1 - 9
Micro business

10 - 99
Small business

100 - 499
Medium business

"AI should be a growth opportunity for every SMB, not only the ones with the strongest security resources. Smaller businesses remain more cautious, as secure adoption is still difficult in practice. If we want more SMBs to benefit from AI, we need to make cyber security simpler to adopt through built-in safeguards, clearer guidance and practical support."

Gustavo Zeidan
Chief Information Security Officer, Sage

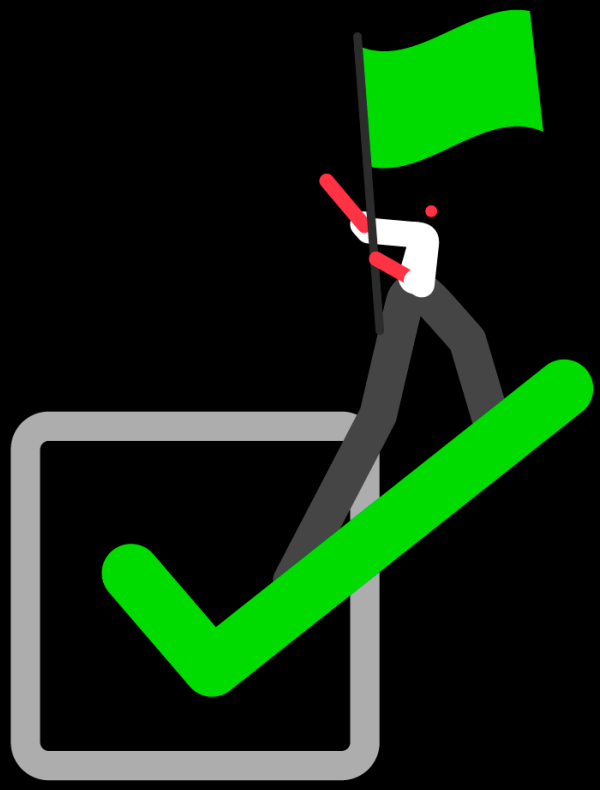
Sage

Table of contents

Sage

Executive summary

SMBs are increasing cyber security investment and accelerating AI adoption. But for many, security practices are still lagging the pace of change, leaving them more exposed as risk expands faster than resilience.



Drawing on a survey of 2,210 SMBs across eight markets, this report examines how small and medium-sized businesses are responding to evolving cyber security challenges, with a particular focus on AI adoption and third-party vendor risk. Cyber security is now a core business priority for small and mid-sized businesses.

In this research, 52% of SMBs say ensuring cyber security and data protection is one of their top priorities for the next 12 months, second only to business growth at 59%, and well ahead of scaling the use of AI at 33%. At the same time, 60% expect to increase cyber security spending, showing clear intent to act.

But for many SMBs, action is still not keeping pace with the risk. Around half report experiencing a cyber incident each year, and proactive security practices remain limited, especially among smaller firms. Only 13% of micro businesses and 21% of small businesses describe their approach as proactive, compared with 48% of medium-sized organisations.

AI is increasing the pressure. It is not creating an entirely new set of risks, but it is making familiar threats faster, more convincing, and harder to manage. Many SMBs are still in the early stages of preparing for AI-related threats, particularly smaller businesses. 84% of micro businesses and 65% of small businesses say they are unprepared or only taking early steps.

At the same time, 22% report having no specific security measures in place for AI applications, rising to 44% among micro businesses.

Third-party SaaS and supply chain risk represent a major blind spot. While SaaS tools are pervasive across SMB ecosystems, 43% of micro businesses do not conduct regular or continuous monitoring of third-party vendors, relying instead on static certifications or one-off checks. This limits real-time visibility into vendor risk and increases the likelihood that security gaps will go undetected until disruption occurs.

The findings point to a clear imperative: SMBs do not need more complexity. They need simpler, more practical ways to move beyond reactive, tool-led security and make risk management part of everyday business.

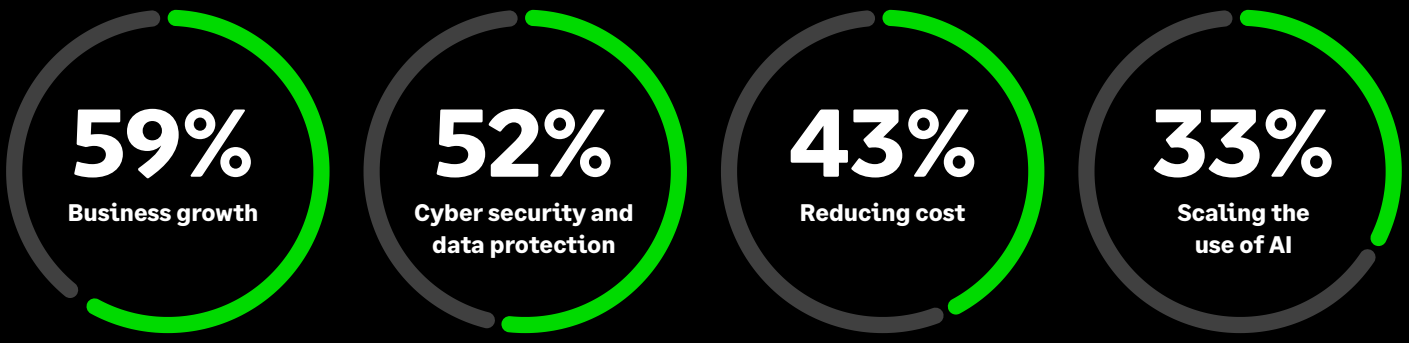
That means building security in from the start, strengthening day-to-day discipline, and focusing on clear ownership, regular monitoring, and employee awareness in ways that reflect the size of the business. Getting this right matters not only for individual organisations, but for customer trust, supply chains, and the resilience of the wider digital ecosystem

Sage

Cyber security is a now core SMB priority—but competing IT demands are stretching budgets

When asked about their top business priorities for the next 12 months, over half of SMBs (52%) cite cyber security and data protection, placing it just behind business growth (59%) and ahead of cost reduction (43%). This signals a clear shift in mindset. Cyber risk is no longer viewed as a purely technical issue, but as a material business concern.

Top business priorities for the year:



Planning security budget increase in the next 12 months:

51% **1 - 9** Micro business

59% **10 - 99** Small business

65% **100 - 499** Medium business

Sage

This intent is reinforced by planned investment. Six in ten SMBs (60%) say they expect to increase cyber security spending in the next 12 months, signalling both recognition of the problem and a willingness to act. However, competing pressures — including cost control and accelerating AI adoption (33%) — mean that progress is uneven.

As a result, while cyber security is clearly rising the priority list, increased spend does not always translate into improved preparedness, helping explain why gaps in confidence, governance and execution persist across the SMB market.

The data points to a growing intent–execution gap. Cyber security matters more than ever, but many SMBs struggle to operationalise it consistently.

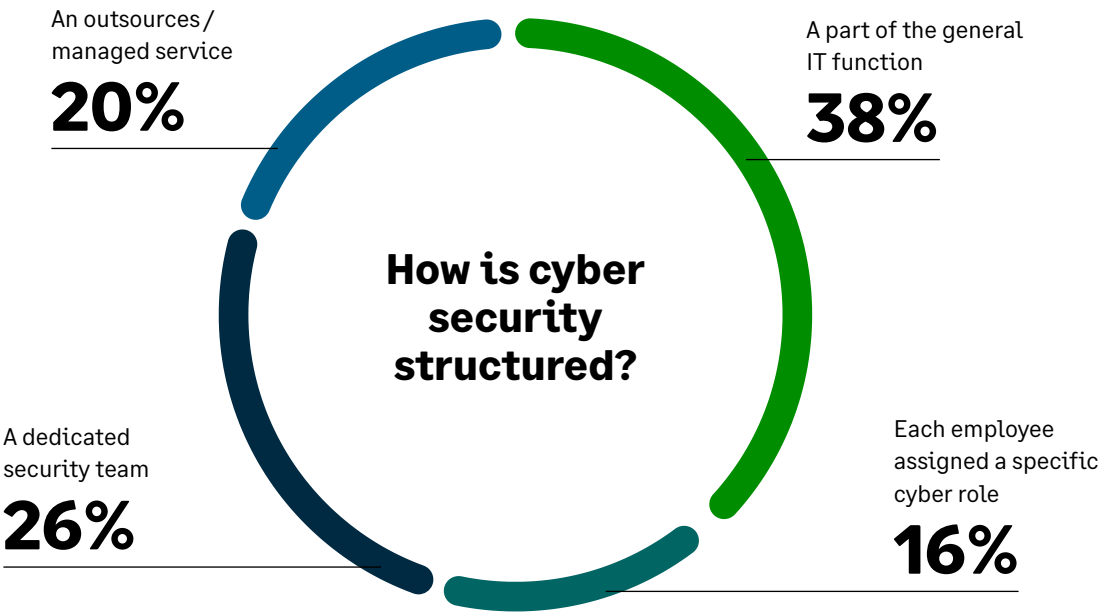
of SMBs say they expect to increase cyber security spending in the next 12 months

Security governance remains informal for most SMBs – limiting the impact of rising investment

For the majority of SMBs (38%), cyber security responsibilities remain loosely defined and embedded within the broader IT function rather than supported by clear ownership, formal review cycles or documented processes.

As a result, security activity is often reactive, triggered by incidents rather than managed as a routine business discipline.

This governance gap helps explain why increased cyber security spending does not always result in stronger preparedness. Without clearer accountability, routine oversight and operational discipline, even well-intentioned investment struggles to deliver consistent risk reduction — particularly as AI and third-party tools increase exposure.



To close this gap, **SMBs need to make security a more consistent part of everyday business**, with clear accountability, regular review and practical processes that can scale over time.

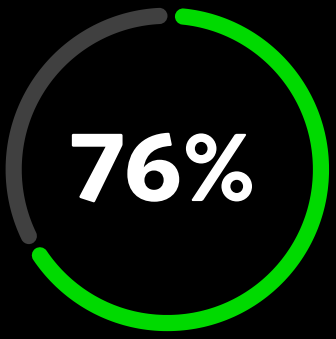
Most SMBs have the right security tools, but struggle to apply them consistently

Core technical controls are now standard across most SMBs, but challenges remain in areas such as tool management, staff training and incident response planning.

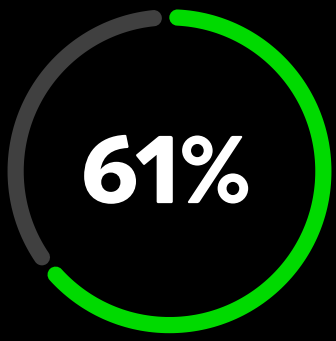
As a result, security maturity depends less on introducing new controls and more on embedding the operational discipline needed to keep existing safeguards effective as the business evolves.

In order to strengthen cyber security posture, SMBs should place greater emphasis on data governance, security controls and transparency. As they scale, this requires more formalised review cycles, clearly defined accountability and consistently documented processes across the organisation.

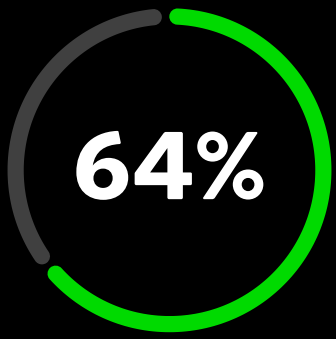
Operational confidence indicators:



regularly review their cyber security

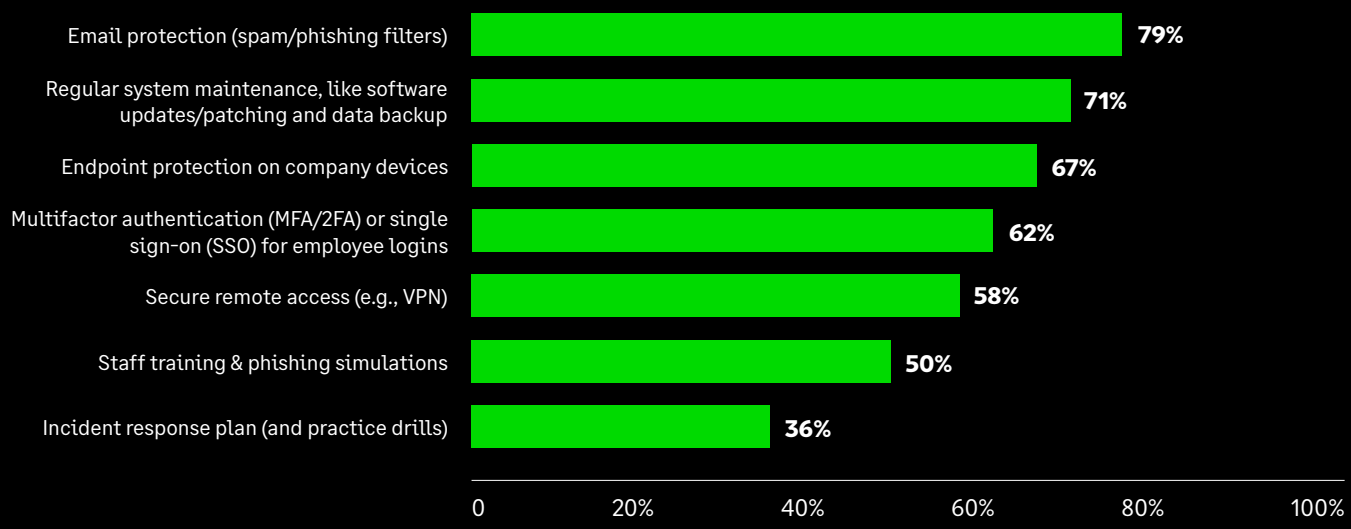


say employees are trained to identify cyber risks



rigorously review third-party security before contracting

Which cyber security measures are currently in place?



Sage

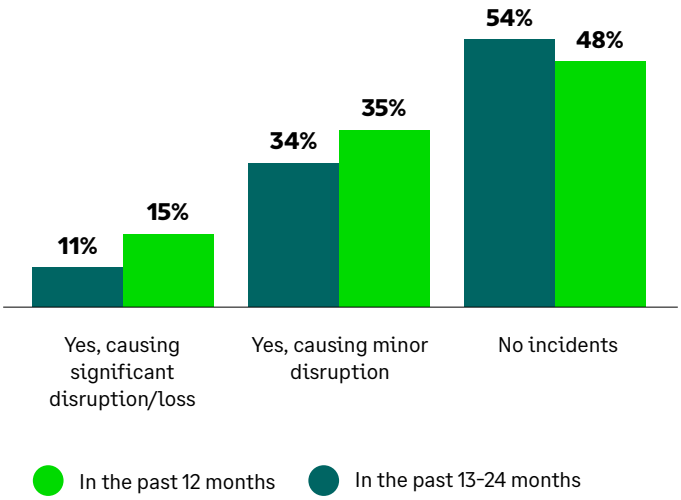
When security remains informal, incidents become disruptive

For SMBs, cyber risk is no longer an occasional disruption. It is an ongoing business challenge shaped by a broader and less predictable mix of threats, from phishing and social engineering to insider risk, third-party exposure and supply chain vulnerabilities.

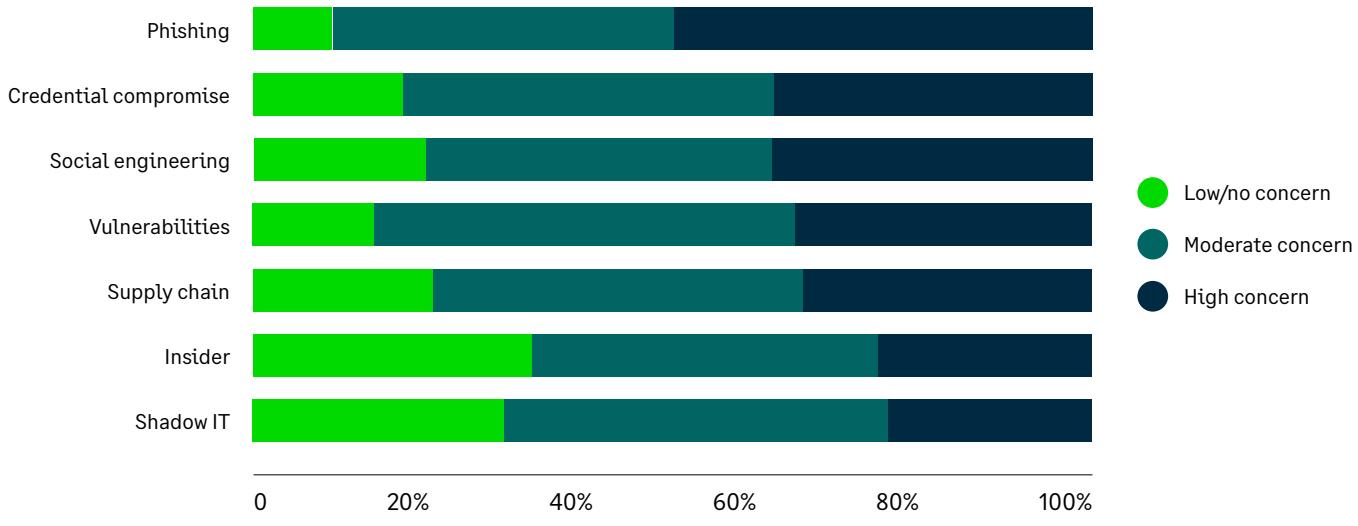
As that exposure widens, resilience depends less on trying to prevent every incident and more on being able to manage disruption well.

That shifts the focus from incidents alone to response quality: how quickly problems are identified, how effectively they are contained and how consistently the business can recover while protecting trust, cash flow and continuity.

Cyber security incidents or data breaches



Concern about each of the following risks



For SMBs, this means putting in place **simple, repeatable ways to spot issues early**, respond quickly, contain the impact and keep the business running when disruption happens.

Rapidly evolving threats and limited visibility are increasing SMB cyber exposure

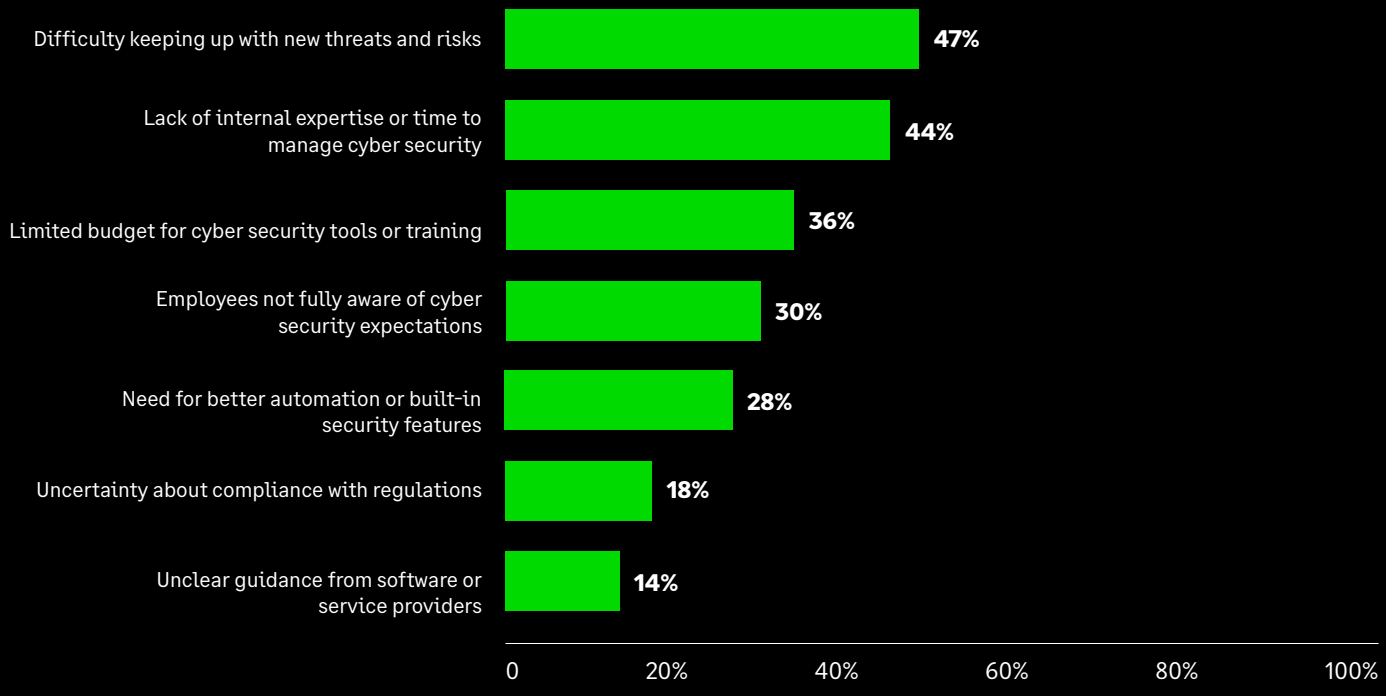
Nearly half of SMBs (47%) identify keeping up with new threats and risks as their primary cyber security challenge.

AI-enabled attacks, more sophisticated phishing and expanding use of cloud and SaaS services are increasing both the speed and complexity of cyber risk — often faster than internal capabilities can adapt.

At the same time, many SMBs lack clear, ongoing visibility into where their greatest exposures lie. Limited specialist skills, competing operational priorities and budget constraints make it difficult to sustain continuous monitoring or structured risk assessment. As a result, cyber risk is often understood in broad terms, but not actively managed day to day.

This combination — rapidly evolving threats and incomplete visibility — significantly increases the likelihood that issues are detected late, prioritised inconsistently, or addressed only after disruption occurs. For SMBs with informal governance and uneven operational discipline, this creates a persistent gap between perceived risk and actual exposure.

Which of the following best describe the main challenges your organisation faces in managing cyber security?



To accelerate progress, SMBs should prioritise solutions that reduce operational overhead, including automation, built-in safeguards, and external support aligned to their resource constraints.

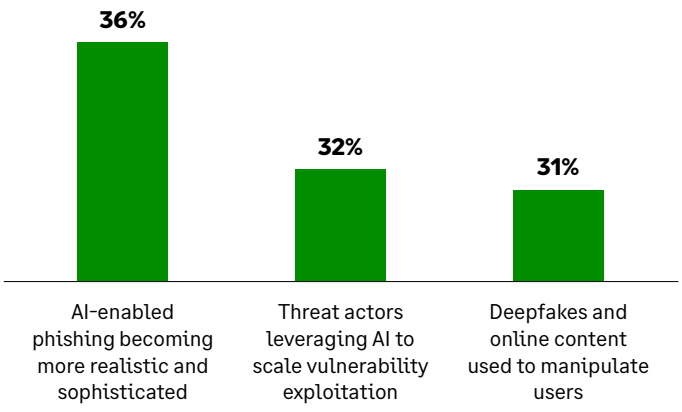
AI-driven threats are evolving faster than SMB security practices

AI is adding pressure to an already challenging cyber landscape, and smaller businesses are the least prepared to keep up.

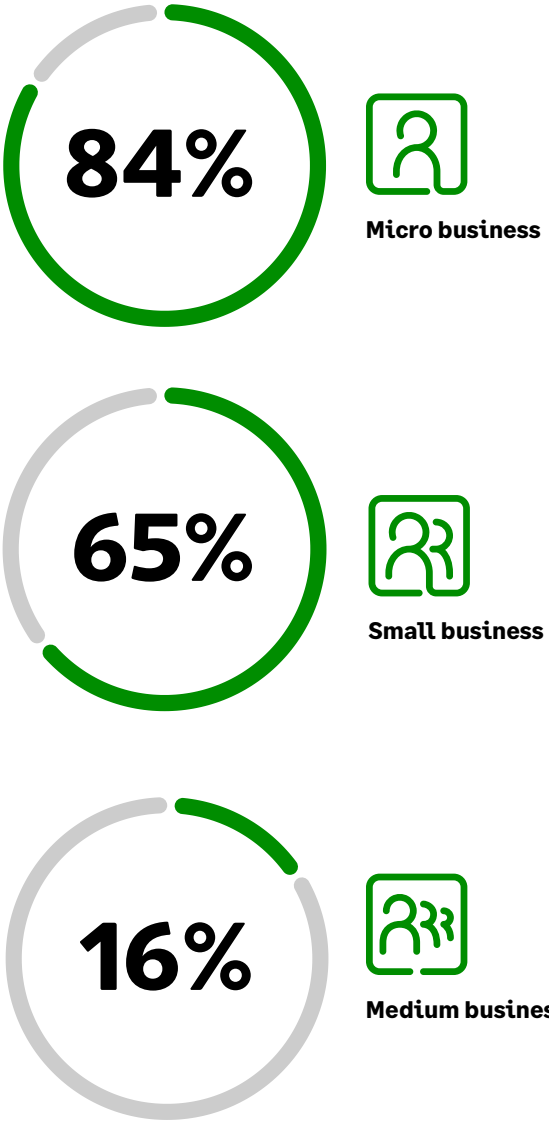
Micro and small organisations face the biggest gaps, with weaker day-to-day oversight, less consistent monitoring, and lower staff awareness leaving them more exposed as AI increases both the speed and scale of attacks. Security practices that may have been enough in the past are becoming less effective as threats evolve faster.

For SMBs, the response should start with the basics: stronger awareness, practical safeguards, and clearer ways to spot and manage risk early. But that is only part of the answer. As AI-related threats evolve, businesses will also need simpler ways to automate routine security tasks, reduce manual effort, and free up limited IT and security capacity to focus on the areas of greatest risk.

Top 3 concerns about emerging AI risks



Not prepared or in the early stages of preparedness for AI-related threats:



For **less mature SMBs in particular, education and awareness remain critical.** Security leaders should prioritise practical, easy-to-adopt measures that help teams recognise and reduce AI-related risk without adding unnecessary complexity.

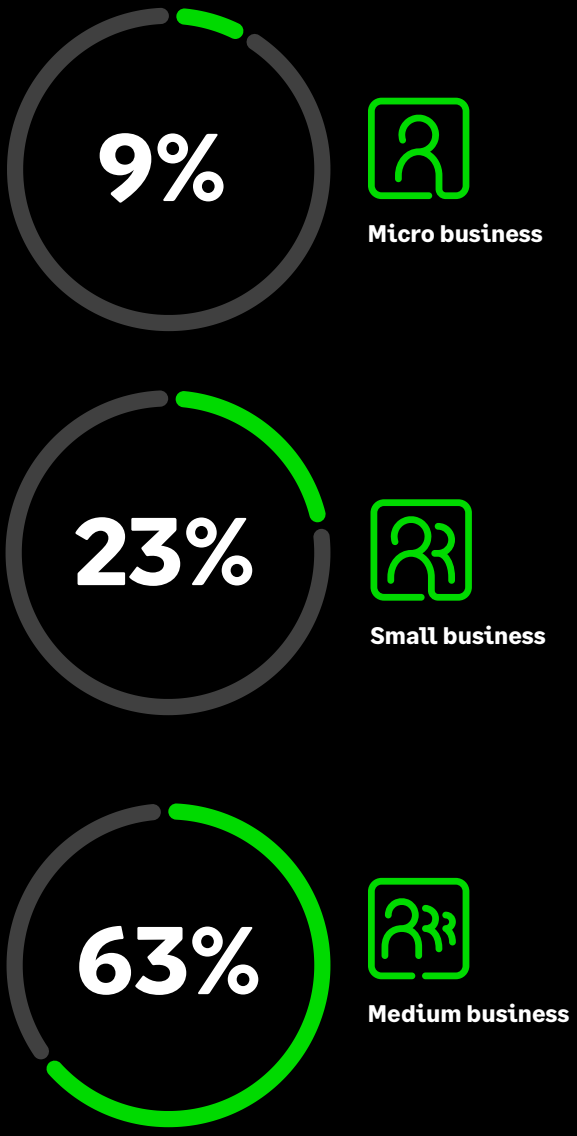
Sage

SMBs pursue AI for opportunity—even as security risk rises

A significant share of SMBs see opportunity in AI while a larger proportion believe AI increases cyber risk. A significant share of SMBs see opportunity in AI while a larger proportion believe AI increases cyber risk. Perception varies by size. Medium businesses are more likely to view AI as an opportunity.

Micro and small businesses approach AI with more caution. This reflects differences in confidence in security controls and governance, rather than ambition.

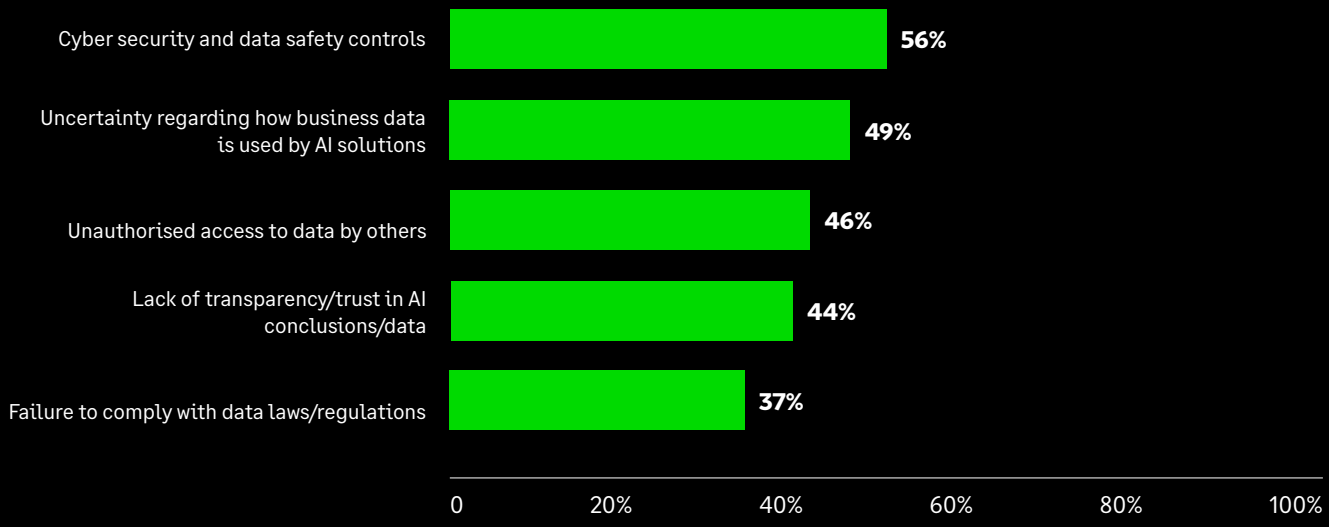
AI seen as business opportunity:



Sage

Concerns exist around data security, governance, and transparency in AI adoption. Without clear visibility into how data is used and protected, many SMBs remain cautious about scaling AI.

Which of the following best describes your primary concerns about adopting or using AI within your business?



As AI becomes more embedded in day to day operations, SMBs need clear visibility over where and how it is being used, alongside defined governance to manage associated risks. This includes identifying AI tools and systems across the business and establishing appropriate oversight, policies and accountability at a leadership level. Without this, the pace of AI adoption can outstrip an organisation's ability to manage risk, increasing exposure rather than delivering value.

SMBs are already laying the foundations for AI regulatory compliance

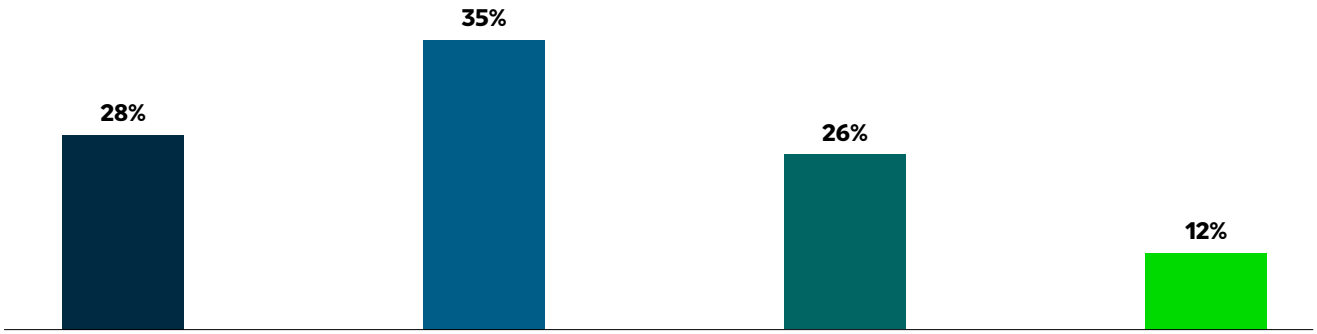
As AI regulations and standards continue to emerge, many SMBs are starting to lay the foundations for compliance.

Frameworks such as national AI regulations and voluntary codes of practice are intended to help organisations translate high-level policy into practical, day-to-day security and governance measures. A growing number of governments are recognising that baseline software and AI security practices need to be widely adopted across the supply chain, not just by large enterprises. Countries such as the UK are focusing on practical, proportionate approaches.

One example is the Software Security Code of Practice and the associated Software Security Ambassadors Scheme, launched as part of the UK Government's Cyber Action Plan. The scheme brings together public- and private-sector organisations — including Sage — to champion adoption of foundational software security principles, share practical implementation experience, and support improved resilience across the economy.

> "SMEs are the backbone of the British economy yet we know many struggle to invest in cyber security at a time when cyber threats are increasing. Improving cyber resilience across the UK is a priority for the government which is why our National Cyber Security Centre has developed the Cyber Action Toolkit to help SMEs boost their cyber defences. We recommend all businesses adopt our highly effective Cyber Essentials scheme which helps protect against common online threats and reduces the chances of becoming the victim of a costly and disruptive cyber attack."
>
> **The Rt Hon Liz Kendall MP, UK Secretary of State for Science, Innovation and Technology**

SMB readiness to comply with AI regulations and assurance standards



Not prepared
Little to no awareness or planning for AI regulations or standards

Getting started
Aware of upcoming requirements; early discussions or planning underway

In progress
Actively developing policies, control, and governance to comply

Well prepared
Processes and safeguards already in place to meet new requirements

For SMBs, initiatives like this highlight a pragmatic path forward: aligning with recognised frameworks, choosing partners committed to secure development, and embedding basic security practices early as AI adoption accelerates.

Sage

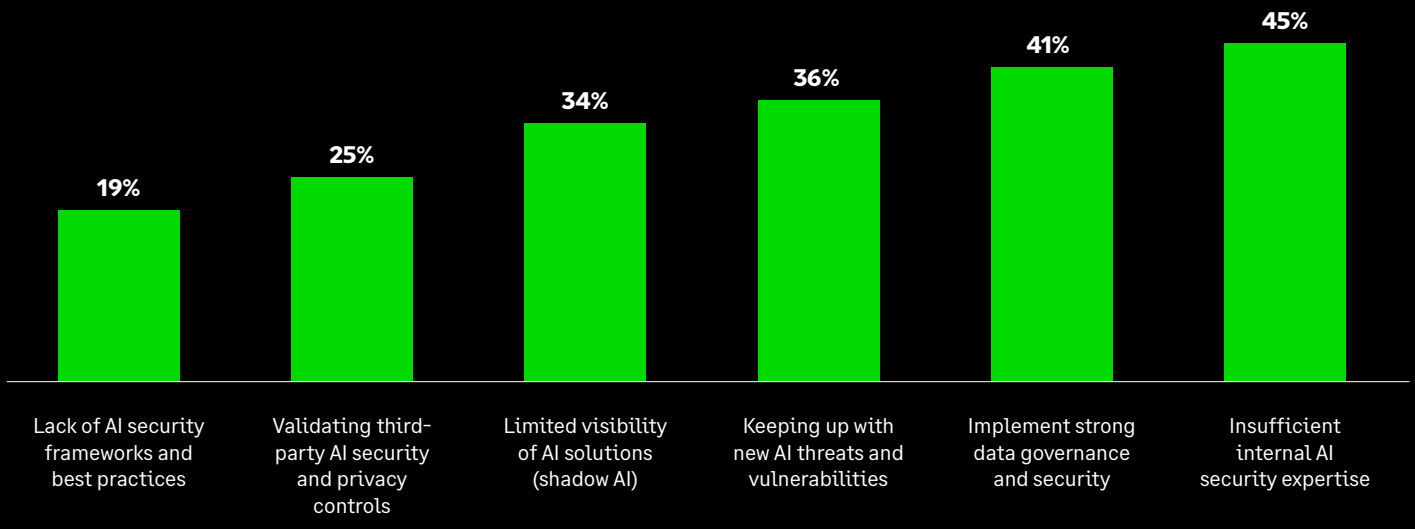
AI security challenges for SMBs centre on skills gaps, data protection and fast-moving threats

AI is exposing a capability gap for SMBs, not just a technology gap. Many organisations are adopting AI faster than they can understand the risks, assess exposure, or judge the security of third-party providers.

This is especially difficult for smaller businesses, where responsibility often sits with a single IT specialist or a generalist team.

Data protection and fast-moving threats add to the challenge. As AI tools rely on access to business and customer data, weak visibility and loose oversight can quickly increase exposure. At the same time, AI is making familiar attacks faster, more convincing and harder to manage, leaving many SMBs struggling to keep up.

Biggest challenges in protecting AI and GenAI applications and infrastructure



For SMBs with limited specialist resource, the priority is to keep it practical: limit AI use to approved tools, set simple rules for what data can and cannot be entered, review AI usage regularly, and lean on trusted vendors or external partners where in-house expertise is limited. That will do more to reduce risk than adding complexity.

Limited monitoring of SaaS vendors leaves many SMBs exposed

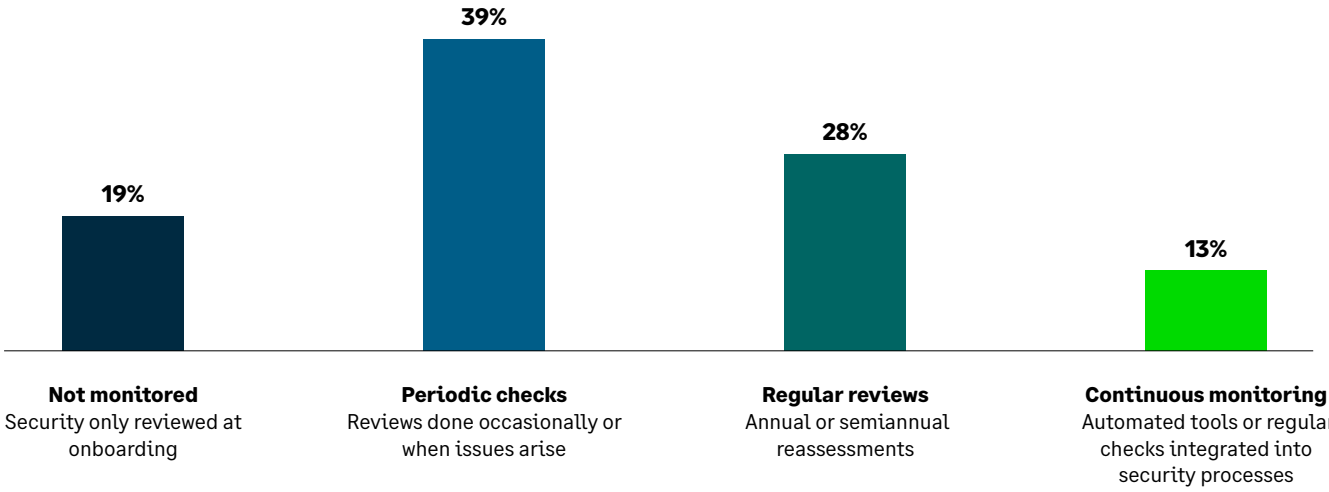
SaaS applications and third-party platforms now sit at the heart of many SMB operations, yet security oversight often remains intermittent.

For many businesses, vendor risk is reviewed at the start of a relationship or when a contract is renewed, rather than monitored continuously. That leaves gaps in visibility, increases exposure, and raises the chance that issues are only identified once disruption has already occurred.

Micro and small businesses are particularly exposed, with a significant proportion reporting little or no regular monitoring of third-party services. As a result, potential issues may go undetected until disruption occurs.

More mature SMBs adopt centralised access controls, clearer user lifecycle management and more regular vendor reviews, improving their ability to identify anomalies and respond earlier. The findings suggest that treating third-party security as an ongoing process — rather than a one-off check — is increasingly critical as SaaS ecosystems expand and AI-enabled tools are introduced via external providers.

Frequency with which SMBs monitor third-party software-as-a-service (SaaS) vendor security?



For SMBs, improving third-party SaaS security starts with better day-to-day discipline: know which tools are being used, control who can access them, remove unused accounts quickly, and look out for unauthorised apps or unusual activity. For smaller teams in particular, a simple, consistent approach supported by trusted vendors or managed services will be more effective than trying to build a complex monitoring model alone.

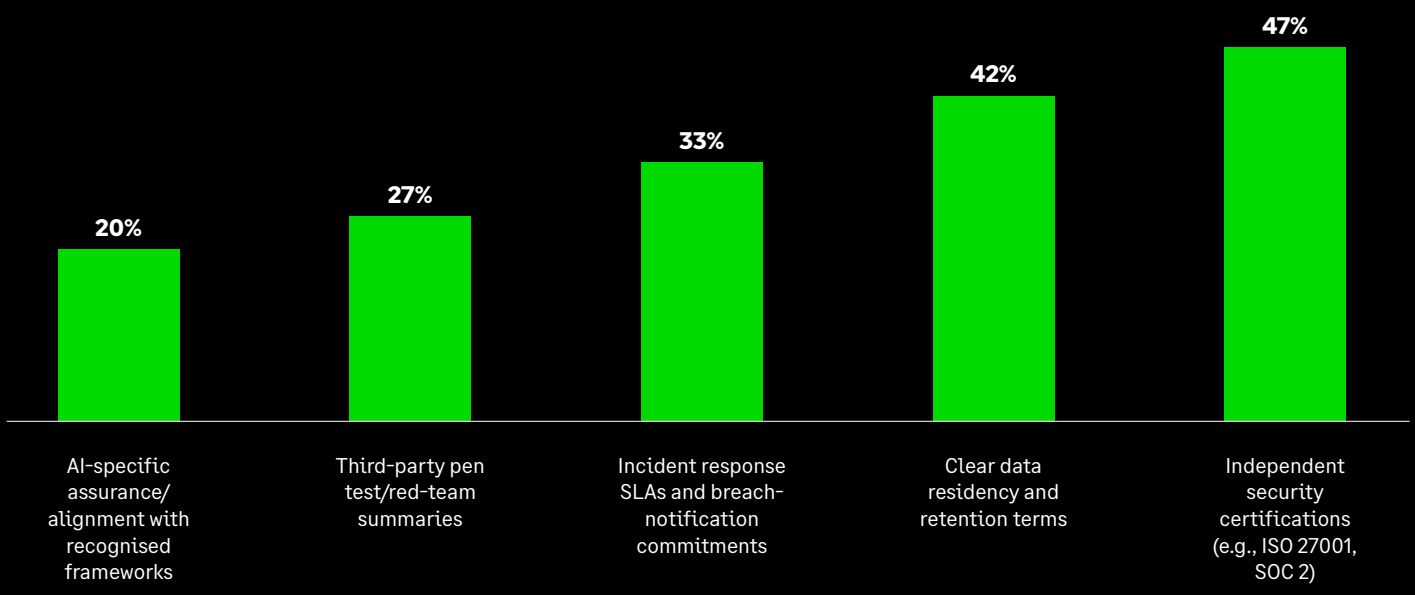
SMBs trust clear, verifiable proof when assessing third-party vendors

As SaaS and AI-enabled services become more embedded in SMB operations, vendor trust increasingly depends on proof that is clear, familiar, and easy to verify.

SMBs place greatest value on independent certifications, transparent data handling, and clear incident response commitments because these provide practical reassurance that core security measures are in place. More technical AI-specific claims may sound advanced, but they are often harder for smaller organisations to assess with confidence.

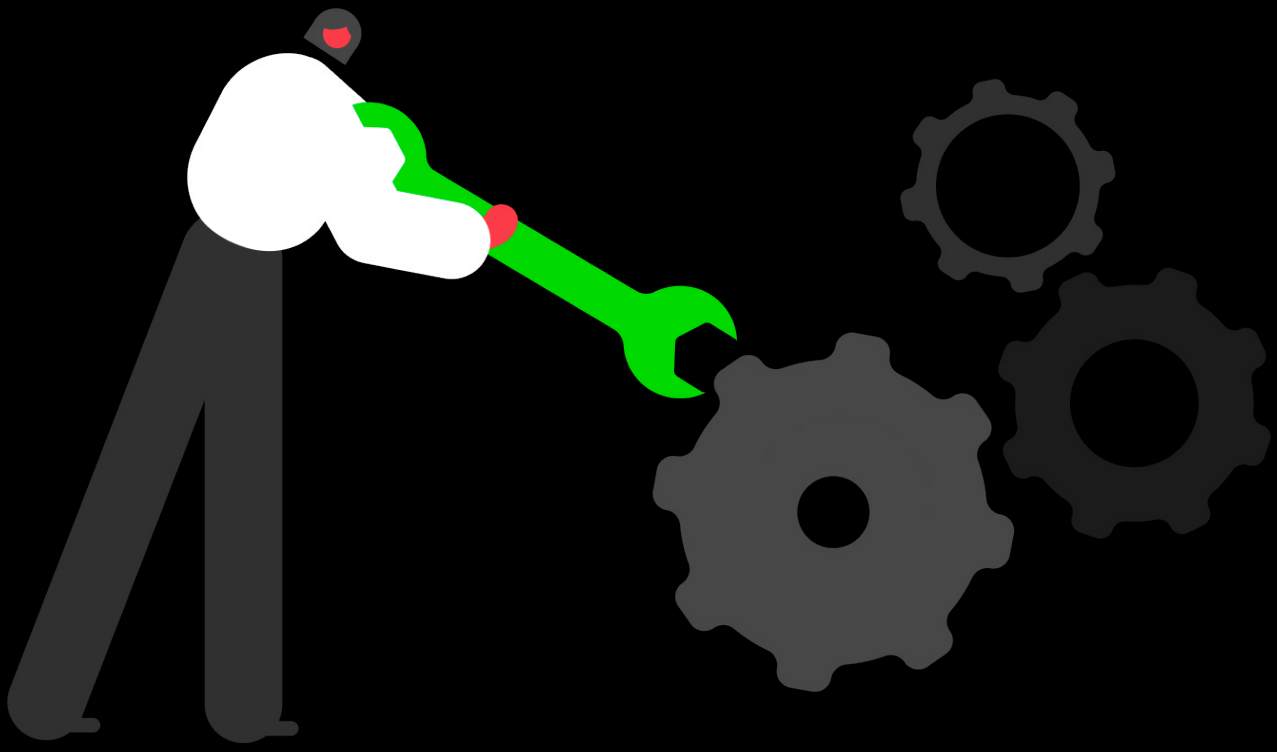
That makes clarity a competitive advantage. Vendors that can explain, in simple terms, how customer data is protected, where it is stored, and what happens if something goes wrong are better positioned to earn trust.

Evidence that builds trust in a third-party vendor's AI security and responsible practices



SMBs should prioritise vendors that provide clear, auditable evidence of how they manage security, and review that trust regularly rather than treating it as a one-off check.

Turning insight into action



Sage

Micro businesses: building resilience with simple, scalable steps

As AI adoption expands, strengthening ownership, review cycles, and basic governance is critical. Actions should remain low-cost and easy to implement, prioritising simplicity and minimal management overhead.

Short-term actions

Cyber security posture

Create accountability: Appoint a security owner and document a simple incident response checklist covering escalation, backups and external support.

AI Security

Secure AI system access: Restrict access to AI systems to authorised personnel, enable simple activity logging, and enforce strong passwords to reduce risks as AI usage grows.

Mid-term plans

Cyber security posture

Build routine discipline: Introduce regular security review covering access rights, software updates. Backups and third-party tools.

AI Security

Define rules and train staff: Formalise data handling rules and access protocols, provide staff training, and build the foundations for scalable AI security.

Long-term considerations

Cyber security posture

Reduce dependence on internal talent: Consolidate and standardise controls, prioritising low-cost, bundled or managed services to reduce operational and financial overhead.

AI Security

Implement oversight practices: Establish basic continuous monitoring and conduct basic vendor AI security checks. Select applications that are trustworthy and committed to security.

Sage

Small businesses: strengthening security through structure and discipline

Small businesses need to structure security processes and AI governance. As AI adoption expands, formalising and consistently applying security practices becomes critical to reduce unmanaged risk.

Short-term actions

Cyber security posture

Formalise risk visibility: Make security reporting regular, confirm who is responsible for key decisions, and ensure incidents and access reviews are discussed at management level.

AI Security

AI asset visibility: Maintain an up-to-date inventory of AI models, agents, datasets, and services. Monitor for unauthorised or shadow AI app usage.

Mid-term plans

Cyber security posture

Professionalise security operations: Apply policies consistently across teams, introduce third-party risk checks before engaging vendors, and rationalise existing tools to reduce complexity.

AI Security

Secure AI interactions: Validate inputs and outputs to prevent prompt injection, jailbreaks, and data leakage.

Long-term considerations

Cyber security posture

Integrate security into business decisions: Embed security into procurement decisions, digital initiatives and expansion plans so risk management evolves alongside business growth.

AI Security

AI incident readiness: Document and test incident response plan for AI failures or breaches. Introduce structured vendor risk management.

Medium businesses: scaling security across the business consistently

Medium businesses have well-structured security - with dedicated roles, proactive management, and formal third-party oversight. The next step is ensuring this maturity scales consistently as digital and AI exposure grows.

Short-term actions

Cyber security posture

Tighten existing controls: Map critical assets and key suppliers, review access rights across teams, and identify overlapping or underused security tools.

AI Security

AI risk management: Formalise an AI security framework that incorporates AI and data visibility, continuous monitoring for system anomalies, and structured vendor risk management.

Mid-term plans

Cyber security posture

Standardise security practices: Apply the same controls and rules across departments, introduce structured vendor reviews, regularly report key risk indicators to management.

AI Security

Regulatory alignment: Ensure AI use aligns with privacy and AI regulations. Integrate AI considerations into existing security assurance frameworks.

Long-term considerations

Cyber security posture

Embed security into corporate governance: Integrate cyber security into procurement, business continuity, and strategic planning so protection evolves in line with organisational growth.

AI Security

Adversarial testing: Test AI systems for resilience against adversarial or red-team attacks.

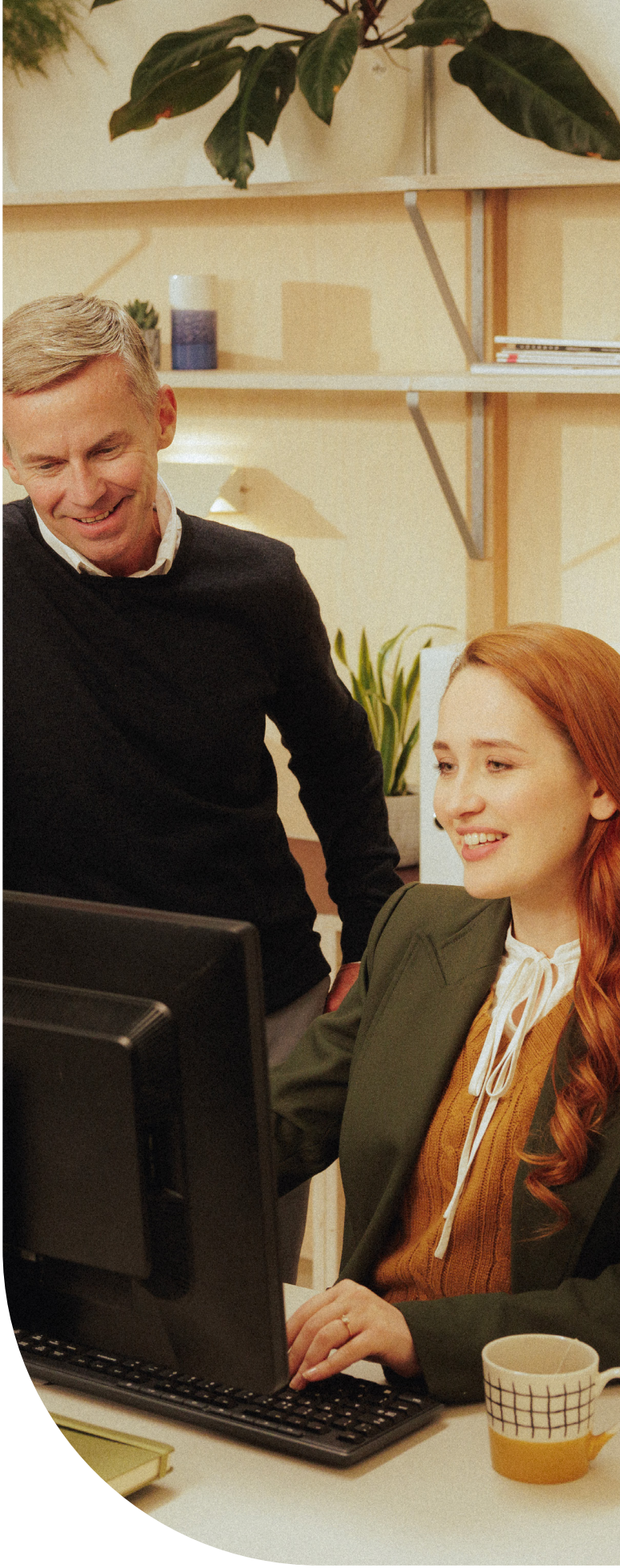
Message from Sage

Sage has long championed small and mid-sized businesses and understands the opportunities and pressures they face. This report shows that cyber security is now a core business priority for SMBs. It sits just behind growth on the business agenda, reflecting how closely cyber resilience is now linked to trust, continuity, and long-term success.

Many SMBs are navigating rising cyber risk with limited time, people, and budget, as AI and third-party technology become more embedded in day-to-day business. They should not have to manage that alone.

At Sage, we are focused on helping SMBs put good security into practice through clear guidance, secure-by-design principles, and transparency around how data is protected and how AI is used. The goal is to enable SMBs to mitigate risks while using technology to fuel growth.

Governments, industry bodies, software providers and vendors should collaborate closely to give SMBs clearer guidance, simpler safeguards, and practical support that fit the realities they face every day.



Sage

Annex: country insights

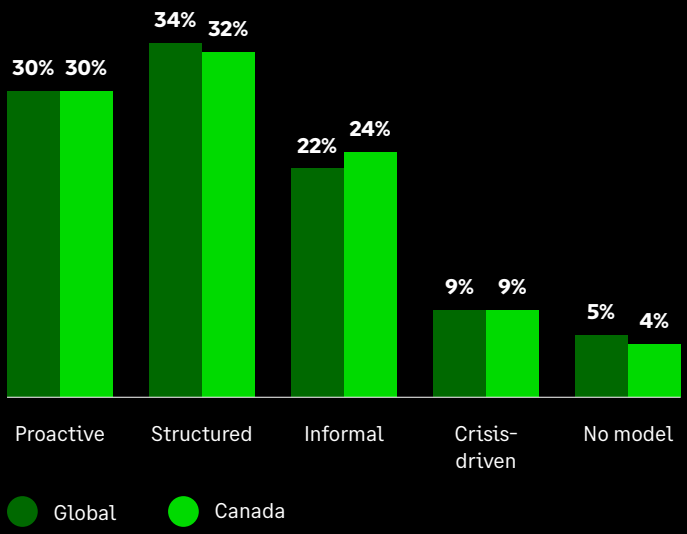
Sage

Canada

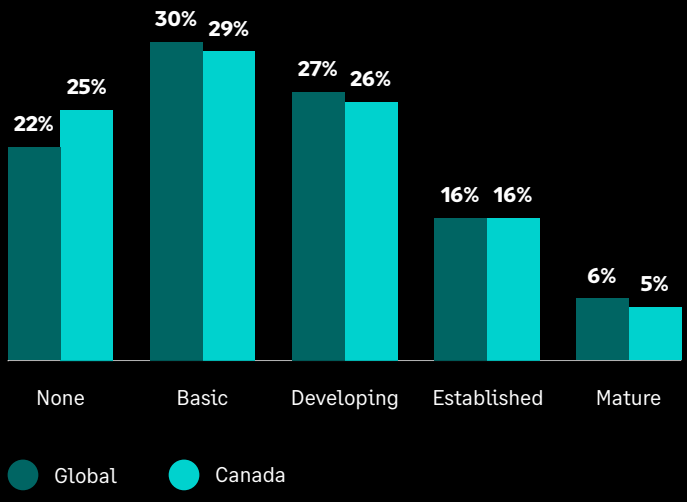
Canada is ahead of the global average on core security measures, giving it a solid baseline in day-to-day protection and helping keep incident levels close to the global average.

The gap opens up around AI readiness. Canada appears less prepared to turn that strong baseline into effective AI security, with weaker adoption of practical safeguards, lower compliance readiness, and the highest reported shortage of AI security expertise. The focus now needs to shift from maintaining the basics to building the skills, oversight, and practical guardrails needed to manage AI-related risk more effectively.

Cyber security management model



Current level of security for AI-powered applications



Cyber incidents or breaches in the past year

	No incidents	Minor incidents, quickly resolved	Incidents causing significant disruption
Canada	55%	33%	10%
Global	54%	34%	11%

Top security measures in place

Canada	86% Email protection	82% Maintenance (Update patching back up)	77% MFA/SSO
Global	79% Email protection	71% Maintenance (Update patching back up)	67% Endpoint protection

Key challenges in protection AI applications

Canada	48% Insufficient AI security expertise	38% Implement strong data security	41% Keeping pace with emerging AI threats
Global	45% Insufficient AI security expertise	41% Implement strong data security	36% Keeping pace with emerging AI threats

Top safeguards for AI risks and threats

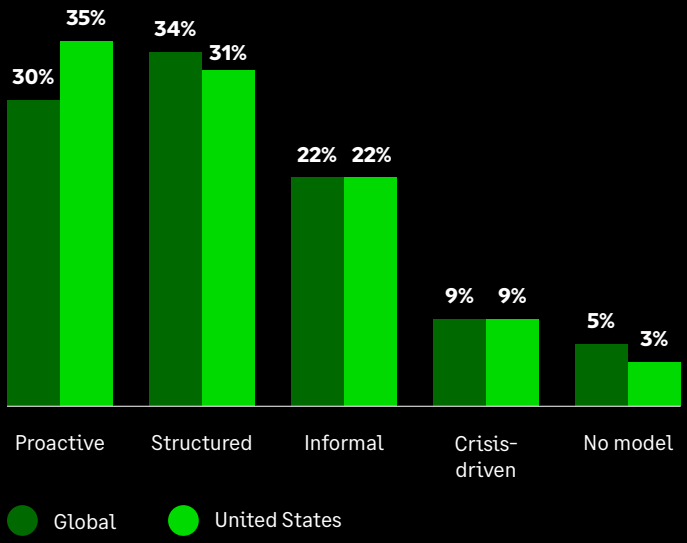
Canada	35% Clear AI use policy	34% Approved AI tools with admin controls	32% Testing AI tools before rollout
Global	41% Clear AI use policy	38% Approved AI tools with admin controls	33% Testing AI tools before rollout

United States

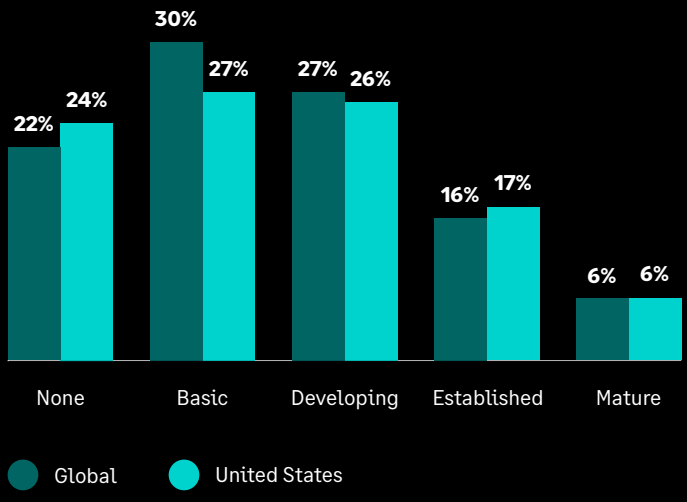
The United States is ahead of the global average in moving from cyber security awareness to more structured day-to-day practice. That gives it a stronger starting point than many markets as AI becomes more embedded in business operations.

The higher share of more serious incidents suggests the focus now needs to shift from building the basics to improving resilience in practice, especially around data security, oversight, and the ability to respond as threats evolve faster.

Cyber security management model



Current level of security for AI-powered applications



Cyber incidents or breaches in the past year

	No incidents	Minor incidents, quickly resolved	Incidents causing significant disruption
United States	55%	32%	13%
Global	54%	34%	11%

Top security measures in place

United States	85% Email protection	71% Maintenance (Update patching back up)	69% Endpoint protection
Global	79% Email protection	71% Maintenance (Update patching back up)	67% Endpoint protection

Key challenges in protection AI applications

United States	43% Insufficient AI security expertise	38% Implement strong data security	38% Keeping pace with emerging AI threats
Global	45% Insufficient AI security expertise	41% Implement strong data security	36% Keeping pace with emerging AI threats

Top safeguards for AI risks and threats

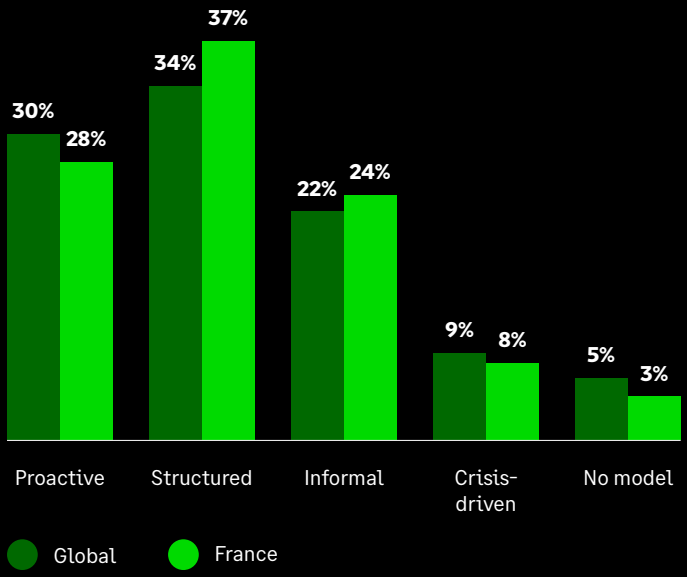
United States	40% Clear AI use policy	39% Approved AI tools with admin controls	34% Testing AI tools before rollout
Global	41% Clear AI use policy	38% Approved AI tools with admin controls	33% Testing AI tools before rollout

France

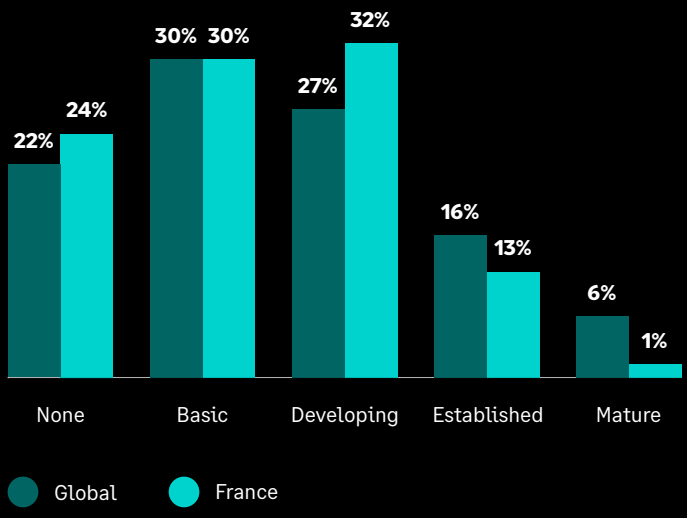
France faces a higher level of cyber pressure than the global average. Core security measures are less widely adopted, the share reporting significant disruption is higher, and AI security maturity remains weaker, with fewer organisations at the more advanced end of the curve. This points to a market where security foundations are less consistent and where the business impact of cyber risk is more pronounced.

The next step is to strengthen both the basics and the ability to manage AI-related risk in practice. Better visibility, stronger data protection, and more structured response readiness will be critical, especially in a market where trust appears to depend heavily on how well organisations can respond when something goes wrong.

Cyber security management model



Current level of security for AI-powered applications



Cyber incidents or breaches in the past year

	No incidents	Minor incidents, quickly resolved	Incidents causing significant disruption
France	51%	33%	15%
Global	54%	34%	11%

Top security measures in place

France	77% Email protection	60% Maintenance (Update patching back up)	69% Endpoint protection
Global	79% Email protection	71% Maintenance (Update patching back up)	67% Endpoint protection

Key challenges in protection AI applications

France	48% Insufficient AI security expertise	43% Implement strong data security	35% Limited visibility of AI tools in use
Global	45% Insufficient AI security expertise	41% Implement strong data security	36% Keeping pace with emerging AI threats

Top safeguards for AI risks and threats

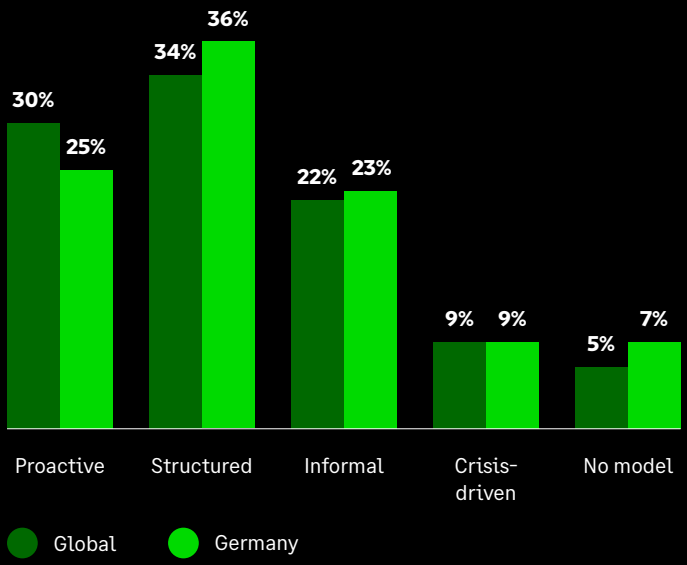
France	42% Clear AI use policy	38% Approved AI tools with admin controls	34% Testing AI tools before rollout
Global	41% Clear AI use policy	38% Approved AI tools with admin controls	33% Testing AI tools before rollout

Germany

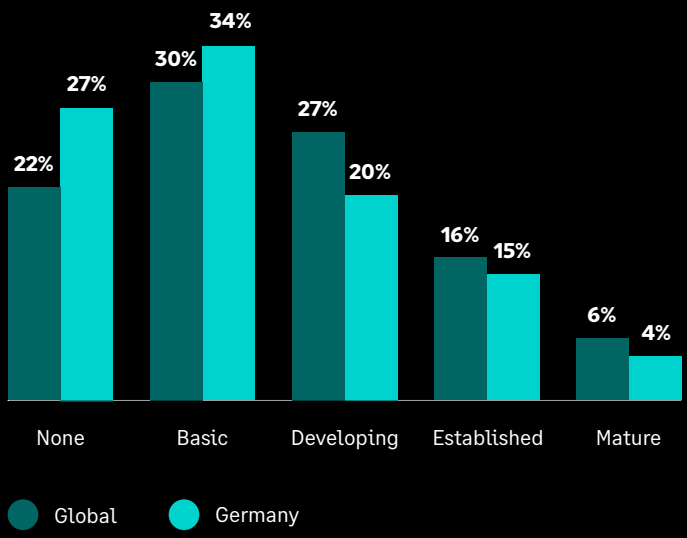
Germany shows a more cautious and compliance-led profile than the global average. Core measures are less widely adopted, proactive management is lower, and AI security maturity remains weaker, with more organisations still at the early stages. Incident levels are close to global norms, so the pressure is less visible today, but the foundations for managing AI-related risk are still underdeveloped.

Germany's priority is to move from caution to practical readiness. Strong concern around data use and limited visibility into AI tools highlights a market focused on control and compliance. The next step is to strengthen practical safeguards, improve visibility into AI use, and make sure caution translates into stronger resilience as AI adoption grows.

Cyber security management model



Current level of security for AI-powered applications



Cyber incidents or breaches in the past year

Germany	54% No incidents	36% Minor incidents, quickly resolved	10% Incidents causing significant disruption
Global	54% No incidents	34% Minor incidents, quickly resolved	11% Incidents causing significant disruption

Top security measures in place

Germany	77% Email protection	68% Maintenance (Update patching back up)	61% MFA/SSO
Global	79% Email protection	71% Maintenance (Update patching back up)	67% Endpoint protection

Key challenges in protection AI applications

Germany	43% Insufficient AI security expertise	39% Implement strong data security	37% Limited visibility of AI tools in use
Global	45% Insufficient AI security expertise	41% Implement strong data security	36% Keeping pace with emerging AI threats

Top safeguards for AI risks and threats

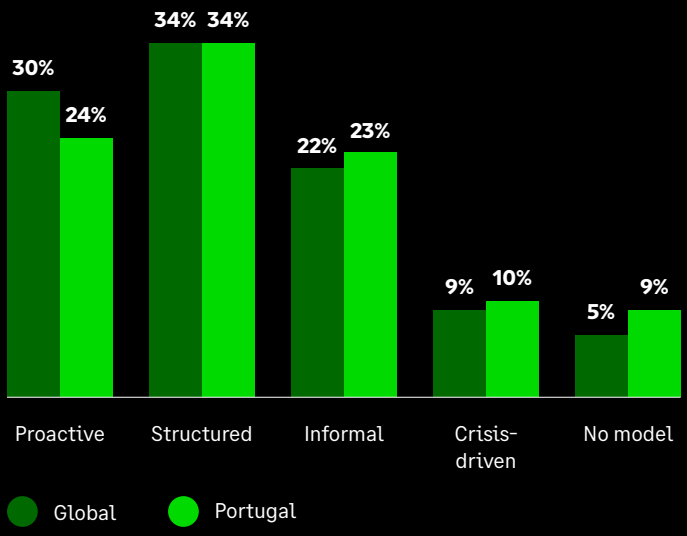
Germany	42% Clear AI use policy	32% Approved AI tools with admin controls	26% Sensitive data protection controls
Global	41% Clear AI use policy	38% Approved AI tools with admin controls	33% Testing AI tools before rollout

Portugal

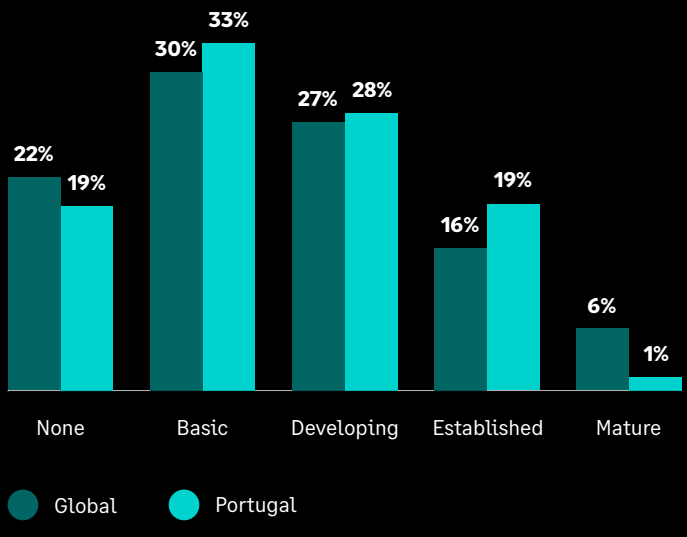
Portugal shows a less mature security profile than the global average. Core security measures are less widely adopted, incident levels are higher, and significant disruption is more common. AI security maturity also remains uneven, with more organisations concentrated at the basic stage and very few reaching mature adoption.

Portugal's challenge is execution. The priority now is to strengthen the basics, reduce uncertainty around AI-related data handling, and build more consistent day-to-day security practice so risk is managed with less disruption. The stronger reliance on independent certifications also shows a market looking for clear external proof of trust as AI adoption grows.

Cyber security management model



Current level of security for AI-powered applications



Cyber incidents or breaches in the past year

	No incidents	Minor incidents, quickly resolved	Incidents causing significant disruption
Portugal	43%	39%	16%
Global	54%	34%	11%

Top security measures in place

Portugal	65% Email protection	65% Maintenance (Update patching back up)	61% Endpoint protection
Global	79% Email protection	71% Maintenance (Update patching back up)	67% Endpoint protection

Key challenges in protection AI applications

Portugal	44% Insufficient AI security expertise	40% Implement strong data security	34% Limited visibility of AI tools in use
Global	45% Insufficient AI security expertise	41% Implement strong data security	36% Keeping pace with emerging AI threats

Top safeguards for AI risks and threats

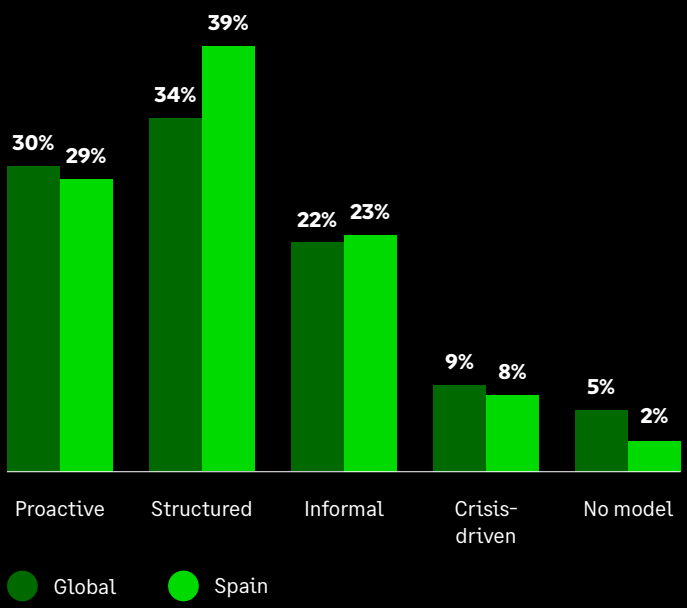
Portugal	43% Clear AI use policy	34% Approved AI tools with admin controls	33% Testing AI tools before rollout
Global	41% Clear AI use policy	38% Approved AI tools with admin controls	33% Testing AI tools before rollout

Spain

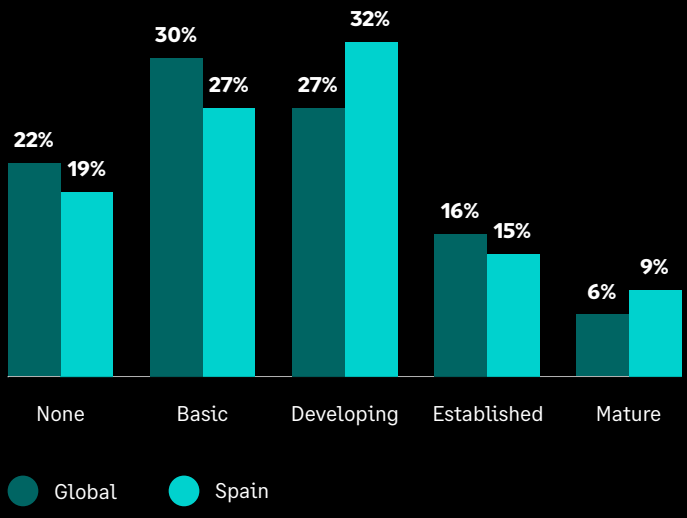
Spain shows a more mature security profile than the global average. Incident levels are lower, structured security management is more common, and AI security maturity is stronger, with more organisations moving beyond the early stages and reaching mature adoption.

Spain's challenge is sustaining that position as AI adoption grows. The priority now is to strengthen protection against human-factor risks, improve visibility into AI use, and close gaps in ongoing third-party monitoring so a stronger starting point is not weakened by blind spots as threats evolve.

Cyber security management model



Current level of security for AI-powered applications



Cyber incidents or breaches in the past year

	No incidents	Minor incidents, quickly resolved	Incidents causing significant disruption
Spain	60%	29%	10%
Global	54%	34%	11%

Top security measures in place

Spain	75% Email protection	72% Maintenance (Update patching back up)	62% Endpoint protection
Global	79% Email protection	71% Maintenance (Update patching back up)	67% Endpoint protection

Key challenges in protection AI applications

Spain	42% Insufficient AI security expertise	36% Implement strong data security	34% Limited visibility of AI tools in use
Global	45% Insufficient AI security expertise	41% Implement strong data security	36% Keeping pace with emerging AI threats

Top safeguards for AI risks and threats

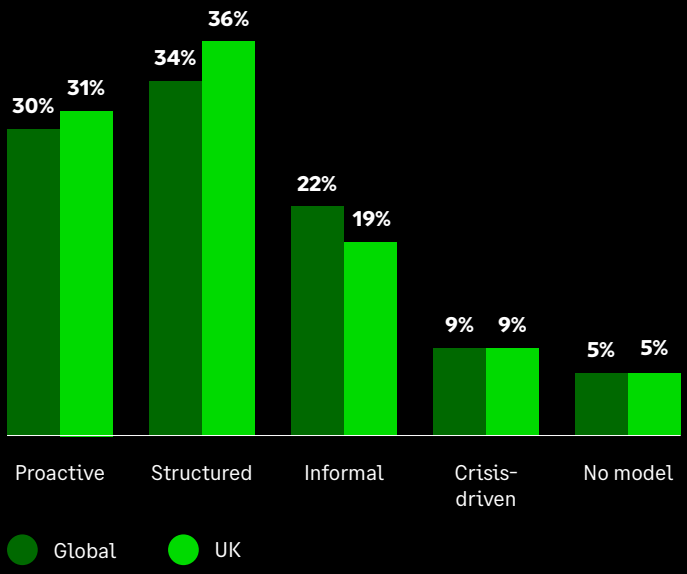
Spain	43% Clear AI use policy	38% Approved AI tools with admin controls	32% Testing AI tools before rollout
Global	41% Clear AI use policy	38% Approved AI tools with admin controls	33% Testing AI tools before rollout

United Kingdom

The United Kingdom stands out for moving further and faster on AI security than the global average. Organisations are more advanced in putting practical safeguards in place, more likely to be using approved tools and formal policies, and further along in building a mature AI security posture. This points to a market that is not waiting to react, but is taking a more deliberate approach to preparing for AI risk as adoption grows.

The priority now is stronger control as AI use expands, especially around data protection, fast-moving threats, and the ability to turn a stronger AI posture into resilience in practice. The slightly higher level of significant disruption also shows that progress on readiness still needs to be matched by consistent execution when incidents occur.

Cyber security management model



Current level of security for AI-powered applications

Cyber incidents or breaches in the past year

	No incidents	Minor incidents, quickly resolved	Incidents causing significant disruption
UK	55%	32%	13%
Global	54%	34%	11%

Top security measures in place

UK	75% Email protection	79% Maintenance (Update patching back up)	67% Endpoint protection
Global	79% Email protection	71% Maintenance (Update patching back up)	67% Endpoint protection

Key challenges in protection AI applications

UK	44% Insufficient AI security expertise	46% Implement strong data security	37% Keeping pace with emerging AI threats
Global	45% Insufficient AI security expertise	41% Implement strong data security	36% Keeping pace with emerging AI threats

Top safeguards for AI risks and threats

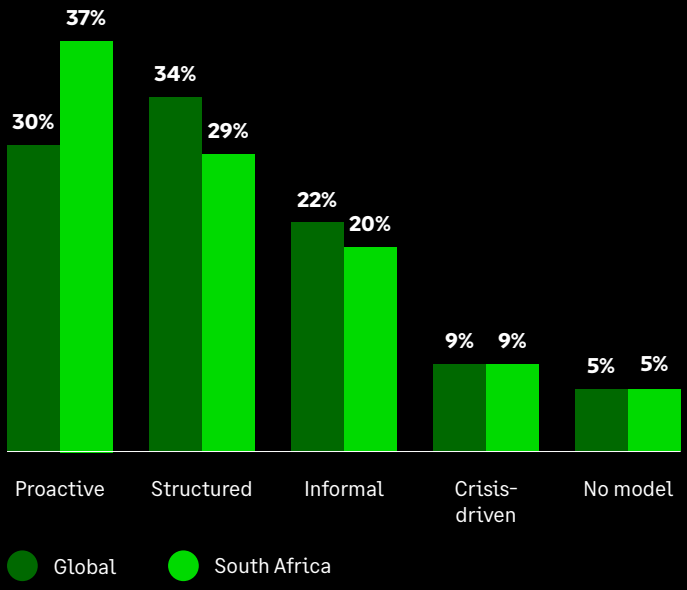
UK	43% Clear AI use policy	45% Approved AI tools with admin controls	38% Testing AI tools before rollout
Global	41% Clear AI use policy	38% Approved AI tools with admin controls	33% Testing AI tools before rollout

South Africa

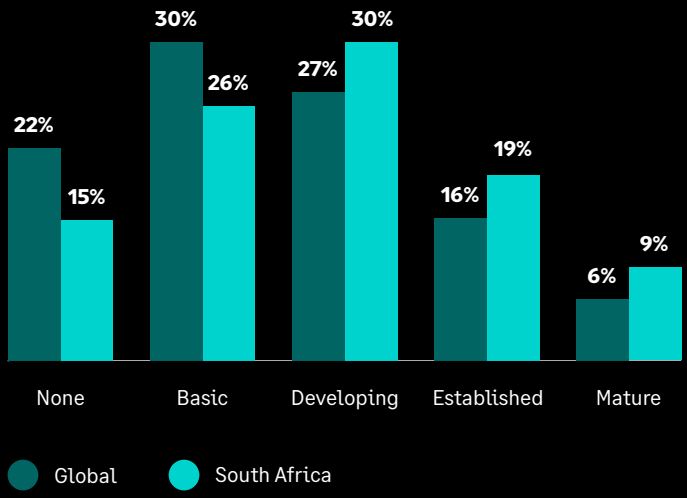
South Africa is ahead of the global average on AI security maturity. Organisations are more likely to have overhauled their approach in response to AI, more advanced in their security posture for AI-powered applications, and stronger on ongoing third-party monitoring. This points to a market that is taking AI risk seriously and putting more practical safeguards in place as adoption grows.

The challenge is to turn that progress into stronger consistency. Core security measures are still mixed, and concerns around data protection and fast-moving threats remain high. The priority now is to close those gaps so a stronger AI posture is matched by more resilient day-to-day security practice

Cyber security management model



Current level of security for AI-powered applications



Cyber incidents or breaches in the past year

	No incidents	Minor incidents, quickly resolved	Incidents causing significant disruption
South Africa	55%	35%	9%
Global	54%	34%	11%

Top security measures in place

South Africa	75% Email protection	74% Maintenance (Update patching back up)	70% Endpoint protection
Global	79% Email protection	71% Maintenance (Update patching back up)	67% Endpoint protection

Key challenges in protection AI applications

South Africa	45% Insufficient AI security expertise	44% Implement strong data security	37% Keeping pace with emerging AI threats
Global	45% Insufficient AI security expertise	41% Implement strong data security	36% Keeping pace with emerging AI threats

Top safeguards for AI risks and threats

South Africa	45% Clear AI use policy	39% Approved AI tools with admin controls	36% Sensitive data protection controls
Global	41% Clear AI use policy	38% Approved AI tools with admin controls	33% Testing AI tools before rollout

Sage

sage.com