changemakers.

Cost to Catalyst:

Reframing Security as the Engine of AI Value

2026 | APRIL

XALIENT

THE DISCUSSION TOPIC

Cost to Catalyst

"You can't transform your business while treating a core part of that transformation as an expense line to be minimised." Forbes 2025

This period of maximum uncertainty and vulnerability is piling pressure onto your business. Yet, AI provides an opportunity to manage immediate pressure and offer avenues for growth. And it is not something for IT alone; security, tech & other business units must align in order to deliver value.

The challenge is, as history has taught a third of organisations who went in blind, AI value is capped by the maturity of your security practices (Forbes 2026). Without the right guardrails, governance & data processes, your ability to deploy AI internally (and particularly, externally) is hugely limited.

The better your security alignment, the greater freedom and trust your AI will have to deliver value. So, as a senior leader, what can you do today to enable AI and deliver value with the right security practices and how can you use this to present security not as a cost but a growth enabler?

REPORT CONTENTS

Contributors

The contributors to this report are senior executives across a variety of large scale organisations and multiple industries. With compelling insights from these industry leaders, this report is a compass for organisations aiming to ensure their AI strategy moves forward securely.

This report identifies the key priorities, strategies, challenges and solutions of this ongoing debate.

Cost to Catalyst: Reframing Security as the Engine of AI Value

AI Exposes Flaws

"AI is not just introducing new risks, it's amplifying the weaknesses we already had." Roundtable Participant

A consistent theme across the discussion was that AI is not introducing entirely new risks, it is exposing and amplifying existing weaknesses. Identity sprawl, poor data classification, legacy infrastructure, and overly permissive access models have long existed within organisations. What AI changes is the scale and speed at which these weaknesses can be exploited. Systems that were "good enough" in a pre-AI world are no longer fit for purpose. As a result, organisations attempting to scale AI are being forced to confront foundational gaps they have historically deprioritised. The reality is clear: AI maturity is directly constrained by security maturity, and without fixing the basics, progress will stall.

Actionable Solutions

"Without the right access controls or classifications, we are just sitting ducks." Roundtable Participant

Strengthen identity and access controls across all entities: Extend least-privilege access to both human and non-human identities to limit lateral movement and reduce exposure.

Implement robust data classification frameworks: Ensure sensitive data is clearly labelled and governed to prevent unintended exposure through AI-driven discovery.

Prioritise legacy risk remediation: Identify and address hidden infrastructure and "unknown assets" that expand the attack surface and undermine AI initiatives.

AI Outpaces Control

"By the time you've done a strategy paper on AI, it's out of date." Roundtable Participant

AI is evolving faster than organisations can plan, govern, or secure it. By the time strategies are defined or governance models are agreed, the technology has already moved on. This creates a growing disconnect between board-level ambition and operational reality. Leaders are under pressure to "do something with AI," yet many lack clarity on use cases, risk appetite, or the infrastructure required to scale. At the same time, adversaries are leveraging AI to increase the speed, volume, and sophistication of attacks, lowering the barrier to entry and widening the gap between attackers and defenders. Organisations are therefore caught in a dual race: adopting AI to stay competitive while simultaneously defending against it.

Actionable Solutions

"AI has dramatically increased the scale and speed of attacks." Roundtable Participant

Adopt adaptive governance models: Move away from static strategies towards flexible frameworks that can evolve alongside AI capabilities.

Focus on high-value, clearly defined use cases: Filter out low-impact or mislabelled "AI" initiatives to concentrate resources where value is tangible.

Invest in continuous monitoring and threat detection: Shift from point-in-time security to real-time visibility across systems and access points.

Questions to Consider:

- *If AI can access everything your users can, how confident are you that access is appropriately restricted today?*
- *Are you building AI on top of weak foundations, and what risk does that create at scale?*
- *How are you balancing the need to move fast with the need to stay secure?*

XALIENT

Cost to Catalyst: Reframing Security as the Engine of AI Value

The Human Factor

"Organisations are uncovering hundreds of applications that they're using and they're not even aware of it." Jaye Tilson, HPE

While much of the AI conversation focuses on technology, the most immediate risk sits with people. Shadow AI is already widespread, with employees using unapproved tools, uploading sensitive data, and experimenting outside of governance frameworks. Traditional controls, such as blocking access, are proving insufficient in a world where employees can easily bypass restrictions via personal devices. At the same time, organisations face cultural fragmentation and AI resistance. Without alignment, education, and trust, organisations risk both underutilising AI and exposing themselves to significant risk. Managing behaviour, not just systems, is now critical.

Actionable Solutions

"You can't mitigate the human factor, people are exposed to AI and can now expose their organisation to its threats." Roundtable Participant

Invest in workforce education and awareness: Ensure employees understand both the value and the risks of AI, particularly around data usage.

Create controlled enablement environments: Provide secure, approved AI tools to reduce reliance on unregulated alternatives.

Foster a culture of transparency and accountability: Encourage teams to share use cases and mistakes to build trust and improve governance.

Security Fuels Growth

"Security is seen as a cost line. Leaders must prioritise how they turn it into a growth enabler" Pragya Madaan, Trainline

Perhaps the most critical shift identified was the need to reframe security at the board level. Too often, security investment is justified only after incidents occur, framed in terms of risk mitigation and cost avoidance. However, this perspective limits progress. AI introduces a new reality: without strong security foundations, organisations cannot scale AI safely or unlock its full value. Security is not just about protection, it is what enables trust, adoption, and competitive advantage. Leaders who successfully reposition security as a strategic enabler, rather than a constraint, will be better placed to move faster, innovate confidently, and differentiate in the market.

Actionable Solutions

"We need to take this to the board in terms of competitive advantage, not just risk." Ian Finn, Tesco

Reframe security investment around value creation: Position security as essential to enabling AI-driven growth, not just preventing loss.

Use real-world scenarios to quantify risk and impact: Bring board-level conversations to life with tangible examples of operational and reputational damage.

Integrate security into AI initiatives from day one: Ensure governance, controls, and risk considerations are embedded early, not retrofitted later.

Questions to Consider:

- *Do you know how your employees are actually using AI today, or just how you expect them to?*
- *Are your controls designed for compliance, or for real-world behaviour?*
- *Are you presenting security to your board as a cost to minimise or a capability to unlock growth?*

changemakers.

XALIENT

Conclusions

AI Value Is Limited by Your Foundations

AI is only as effective as the environment it operates in. Organisations looking to scale AI are quickly discovering that weak identity controls, poor data governance, and unresolved legacy debt act as hard constraints on progress. Without addressing these fundamentals, even the most promising AI initiatives will struggle to move beyond pilot. The real differentiator is not how quickly you adopt AI, but how prepared your organisation is to support it at scale.

Speed Without Control Creates More Risk Than Value

The pace of AI is forcing organisations to move faster than their governance models can keep up. While there is pressure to act, moving too quickly without the right guardrails increases exposure, both operationally and reputationally. At the same time, slowing down too much risks falling behind competitors. The challenge for leaders is not choosing between speed or security, but building the capability to achieve both simultaneously through adaptive governance and continuous oversight.

Security Is the Unlock for AI, Not the Barrier

The most important shift identified is one of mindset. Security can no longer be positioned purely as a cost or constraint; it must be recognised as the enabler of AI-driven growth. Organisations that successfully make this shift will be able to move faster, build trust internally and externally, and unlock new opportunities with confidence. Those that don't will remain stuck, limited not by the potential of AI, but by their ability to use it safely.

COST TO CATALYST: REFRAMING SECURITY AS THE ENGINE OF AI VALUE

The Change Makers Club is a progressive, dynamic and forward-thinking group of senior-decision makers from large-mid scale companies, driven to consolidate and empower change within their industries. Each and every member of the club is a passionate believer in sharing insights to overcome obstacles and break boundaries.

https://www.changemakersclub.com

Xalient is a global boutique driven by a passion for exceptional service and world-class delivery. They excel in the convergence of identity-driven security and networking, enabling enterprises to accelerate time to value with greater agility, stronger cyber resilience, and lasting business impact.

Xalient's global advisory, professional, and managed services teams set them apart—bringing deep expertise, a proven track record, and a relentless focus on understanding and guiding their customers to deliver faster, tangible outcomes. As an independent and innovative organisation, they specialise in connecting users and devices to applications and data—securely and efficiently.

Thank you to our thought leaders for the session:

Jaye Tilson, Chief Technology Officer, HPE

Glenn Wiseman, Business Development Director, Xalient

Stephen Amstutz, Director of Innovation, Xalient

AUTHORS

James Harris
Club Founder

George Whittington
Club Director