Investment Insights

Our monthly look at what's driving global markets

Waiting for God(ot)
The greatest market questions remain unresolved

Investment in the drone age
A revolution in modern warfare poses questions for portfolios

Cheap attacks, costly lessons
AI is reshaping cyber risk and corporate governance

Issue 57 | August 2026

Quick take
In this month's issue

Waiting for God(ot)
The greatest market questions remain unresolved

Markets remain caught between optimism and uncertainty, with the Iran conflict, AI investment, central bank policy, and UK politics awaiting resolution.

The AI spending boom continues, but questions remain over funding, profitability and how quickly businesses will generate returns from these investments.

Despite uncertainty, demand for AI infrastructure remains strong, creating opportunities for long-term investors willing to look beyond short-term volatility.

Central banks are taking a cautious approach to monetary policy as they balance persistent inflation against weak economic growth.

In this environment, diversification and disciplined active management remain key to navigating market swings and capturing long-term opportunities.

Read the full story on page 3.

Cheap attacks, costly lessons
AI is reshaping cyber risk and corporate governance

AI is making cyber attacks cheaper, faster, and more convincing, increasing the financial and operational risks facing businesses.

Recent attacks have shown how weaknesses in suppliers and third-party partners can quickly disrupt operations and damage company value.

Strong cyber resilience is becoming a board-level responsibility, requiring better oversight, regular testing, and closer scrutiny of critical partners.

At the same time, AI is strengthening cyber defences by helping companies detect threats, prioritise risks, and respond more quickly to attacks.

For investors, businesses that treat cyber security as a strategic priority are likely to be better placed to protect long-term value.

Read the full story on page 7.

Investment in the drone age
A revolution in modern warfare poses questions for portfolios

Modern warfare is being transformed by drones, AI, cyber capabilities, and space-based technologies, creating new opportunities and challenges for defence investors.

Recent conflicts show that while low-cost autonomous systems are reshaping the battlefield, conventional military strength and advanced weapons remain essential.

Defence spending is rising as countries replenish depleted stockpiles and invest in more agile, technology-driven capabilities.

Established defence contractors are well placed to benefit by combining innovation with their manufacturing scale, expertise, and government relationships.

For investors, the greatest opportunities currently lie not in drones themselves, but in the companies developing the technologies and systems that support this new era of warfare.

Read the full story on page 5.

Snapshot
The global economy and markets

Key facts and figures from around the world, including the value of experience in an ageing workforce, falling electric vehicle sales, rising renewable electricity generation, higher chocolate prices, and another surge in European gas prices. Also features longer-term trends across global equities, bonds, and commodities.

Find out more on page 9.

Waiting for God(ot)
The greatest market questions remain unresolved

John Wyn-Evans, Head of Market Analysis

Ancient Greek playwrights, when in need of a conclusion, often used the *deus ex machina*: a god winched down to resolve the plot.

With broader indices struggling for direction, do we need a higher force? Usually, that force takes the form of government or a central bank. The problem is they usually intervene when a crisis is at hand, and it would be churlish to invoke a crisis to break the current logjam.

The same themes keep recurring: the Iran War; AI optimism and pessimism; central bank policy; market-crisis fears; and UK fiscal politics – and they remain far from resolved.

The great gulf

Ships and commodities remain trapped in the Persian Gulf with the ongoing Strait of Hormuz closure.

Any commentary comes with the caveat that events may have moved on by the time of reading. Still, the sticking points are clear: the US, Gulf states and most of the world want free passage through the Strait of Hormuz, while Iran sees the threat of closure as both a means of leverage in negotiations and a possible source of future income. The US is determined to neutralise Iran's nuclear threat; Iran is loath to comply.

The global economy has cruised relatively unscathed since the war began back in February, risking complacency. Oil consumers drew on strategic reserves, but these have dwindled. Energy source pivots and a modicum of privation are the easy wins that one might describe as trimming fat, but we're getting closer to the muscle now.

So why do markets remain relatively calm? The consensus is that neither side has the appetite for prolonged hostilities as the financial and political costs rise, and the US is rumoured to be running low on key ordnance.

BCA Research's credible 'oil price collar' theory sees Brent crude trapped between $70 and $100 a barrel. At the lower end, tensions tend to rise as the political and economic costs fall; as prices approach the upper end, escalation gives way to de-escalation as the costs rise again. That concept, albeit a fragile one, seems to be holding.

Mismatched expect-AI-tions

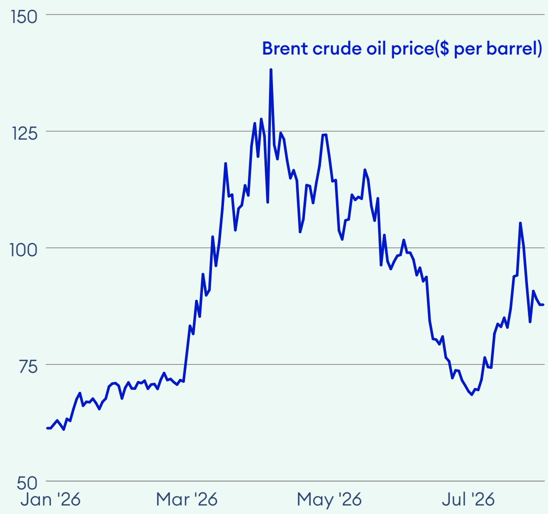
Amara's Law says we tend to overestimate a new technology's short-term effect and underestimate its long-term impact. Generative AI is showing this today, with extreme consequences for certain share prices.

The AI push is largely driven by frontier large language model (LLM) developers (think ChatGPT, Claude, or Google Gemini) and the 'hyperscalers' building the data centres needed to train and run them. LLM funding has come largely from private equity backers.

Hyperscaler spending has so far been funded largely by operating cash flow, which is massive for companies such as Alphabet, Microsoft, Meta and Amazon (with Oracle, of the Big 5, being the notable debt-funded exception). The numbers are mind-boggling: annual capex is forecast to rise from $224bn in 2024 to around $700bn this year and $900bn in 2027.

Figure 1.1: The crude collar

Brent crude has remained trapped in a relatively narrow range as markets anticipate the Middle East conflict will de-escalate.



Source: LSEG, Rathbones

Problem number one: this level of capex is now outrunning cash flow generation. This leads to massive equity issuance ($85bn for Alphabet, for example). It also prompts huge debt issuance (more than $200bn so far in 2026 in public markets and potentially the same again in private markets and through the backing of special-purpose off-balance sheet vehicles).

Problem number two: will all this spending generate a return? It must beat the cost of capital and, ideally, match the returns from existing operations. That is a high bar for hyperscalers, whose exceptional performance has been built on scalable, 'capital light' business models where the majority of every dollar of extra revenue turns into profit.

Problem number three: who's paying for the service? Engagement with LLMs has risen exponentially, but most users are not paying for them. Revenue is mainly coming from companies. Anthropic's record revenue growth has yet to translate into a sustainable profit.

Billing has shifted from an 'all you can eat' basis to a 'per token' or 'per task' model earlier this year. As invoices rose, usage was curtailed or switched to cheaper models for less onerous tasks, many of which are based in China, which is another concern.

This makes for a difficult short-term market. Especially as ownership of the shares involved is meaningfully funded by borrowed money and by leveraged exchange-traded funds and options, all of which exacerbate short-term volatility. The forced liquidation of positions by a hedge fund, ironically called Situational Awareness, at the end of July now seems to have been a key contributor to recent gyrations.

Our central view today is that both the frontier model builders and the hyperscalers are committed to their growth paths. We think the demand for computing power will continue to rise as companies and individuals learn to integrate AI-based solutions productively into their operations and lives, especially if it becomes cheaper (as in Jevons' Paradox). But it will not happen linearly.

“Engagement with LLMs has risen exponentially, but most users are not paying for them”

“With underlying economies weak in both the UK and Europe and President Trump marking Warsh's homework, policymakers remain reluctant to increase interest rates”

For longer-term investors, swings from overoptimism to unmerited pessimism create investment opportunities for active managers.

Central bankers sit on their hands

The latest central bank meetings produced no changes to monetary policy. The new US Federal Reserve chair, Kevin Warsh, has made his committee's intentions less clear and allowed markets to set rates. Markets have duly obliged, selling off long-dated Treasuries and pushing yields back to 2007 levels.

In the UK, despite a 6-3 vote to leave the base rate at 3.75%, one more voter joined the 'hawks' in July. Yet the tone of accompanying statements was interpreted as relatively dovish. The European Central Bank's message fell somewhere in between.

With underlying economies weak in both the UK and Europe, and President Trump marking Warsh's homework, policymakers remain reluctant to raise interest rates. Policymakers are largely 'looking through' the war-related inflationary pressures given that: 1) they are the result of a supply shock that is not readily countered by monetary policy; and 2) there are limited 'second round' effects, such as higher wage demands. That said, markets still see a reasonable chance of rate hikes later this year.

Conclusion: diversification pays off

Current sentiment swings, amplified by leveraged trading vehicles and strategies, make it easy to look like a hero one day and a failure the next. A diversified portfolio provides a more stable ride and keeps us focused on longer-term investment and planning goals. We still take bigger directional bets where conviction is high, and continue to filter markets for opportunities. AI-related winners are likely to proliferate, including in areas not yet apparent, as adoption of this technology remains in its infancy.

Many media stories about extraordinary gains (or losses) probably reflect leverage and/or poor risk management. We do not borrow money to juice returns, and we remain attentive to portfolio volatility relative to agreed benchmarks as stewards of clients' hard-earned wealth.

Investment in the drone age
A revolution in modern warfare poses questions for portfolios

Claire Titmarsh, Equity Analyst

Breakneck technological development has transformed the battlefield – and therefore the risks and opportunities for portfolios. But for all the investment potential in upstart defence-technology companies, technological advance has far from destroyed the investment case for established players.

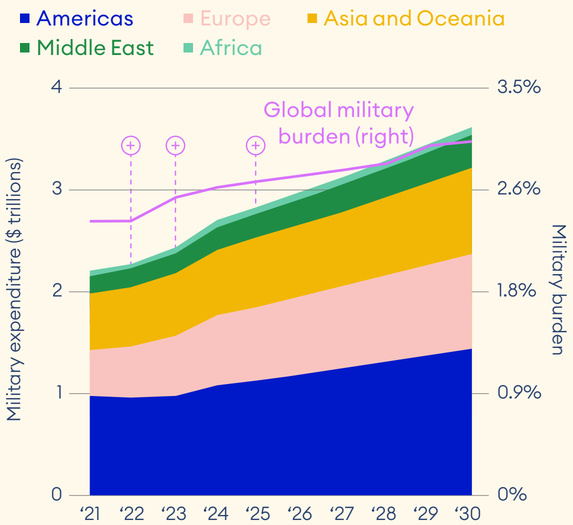
The interminable war in Ukraine increasingly shows modern warfare as a contest of endurance rather than of rapid battlefield advances. Militaries are struggling to break the deadlock, as technological innovations are quickly replicated.

Drones are central to this. Both sides have deployed vast numbers of inexpensive Unmanned Aerial Vehicles (UAVs) to target tanks, logistics hubs, ships, and even energy infrastructure. This means precision targeting – the ability to strike with pinpoint accuracy – is no longer exclusive to advanced militaries.

Continuous drone and satellite surveillance has also greatly increased battlefield transparency, heightening the need for concealment and deception. As both sides seek to counter each other's drones, electronic warfare techniques such as jamming, AI-powered targeting, and autonomous navigation have become crucial. Ukraine shows one scenario for future fighting: attritional warfare – trying to win by gradually wearing your opponent down – that's dominated by drones.

The Iran War shows another scenario: asymmetric warfare. Iran has relied on swarms of low-cost drones and missiles. That forced defenders to use up interceptors worth millions per shot, at a high overall cost. This means the economics of defence, as well as the tactics, need rewriting.

Figure 2.1: Rearming the world
Military spending has risen sharply since 2021. Military burden (the share of GDP devoted to defence) is also increasing and is forecast to continue rising.



Source: Bloomberg, Rathbones

Innovation across the defence industry

Drones capture the most attention, but we see innovation everywhere. Spending on software is growing fast, driven by factors such as complex planning for missions, cyber warfare, and using AI to support decisions. Battles over cyber security could challenge drones as they move from models operated by a person to autonomous versions.

In the twentieth century, wars moved into the air. In the twenty-first, they could move into space. For example, low-Earth-orbit satellite constellations mean a metamorphosis in space-based intelligence, surveillance, and reconnaissance. Modern militaries depend on satellites for GPS navigation, intelligence gathering, secure communications, and missile early-warning systems.

Military aircraft, ships, and armoured ground vehicles are being retrofitted with sensors, processing, and electronic warfare capabilities to create a connected, network-centric battlefield, where people can see their present situation more easily.

Meanwhile, autonomy is spreading across the combat zone – and beyond. Uncrewed surface vessels are emerging. Ground robots are used for resupply and casualty evaluation, or to carry mounted weaponry.

Traditional military capability still matters

Recent conflicts highlight the evolution of warfare. But the US and Israeli strikes on Iran show conventional superiority still matters. Their airpower rapidly degraded Iran's military infrastructure. Critical advantage still lies in precision strikes, advanced intelligence, and using integrated networks to hit targets.

And humans are still part of the picture. But to cut costs and reduce casualties, militaries are shifting to hybrid forces, where humans and drones are combined. Crewed platforms act as command centres, while uncrewed assets handle the riskiest tasks. This extends the reach of aircraft, ground vehicles, and warships – if people aren't put at risk, militaries can be bolder.

For example, the UK's Defence Investment Plan, announced in June, details how the Royal Navy is becoming hybrid. At least six Common Combat Vessels (CCVs) will act as motherships alongside crewed frigates. People on the CCVs will coordinate uncrewed fleets.

Affordable air defence

Integrated air and missile defence is vital on the battlefield. It also protects populations and infrastructure, such as airports and power grids, from missiles and UAVs. Saturation attacks, in which massed volleys of cheap projectiles seek to overwhelm advanced defences, are pushing defence systems towards cost-effective models with different layers of protection. That could include affordable interceptors, electronic jamming, and lasers that neutralise drones at minimal cost per shot.

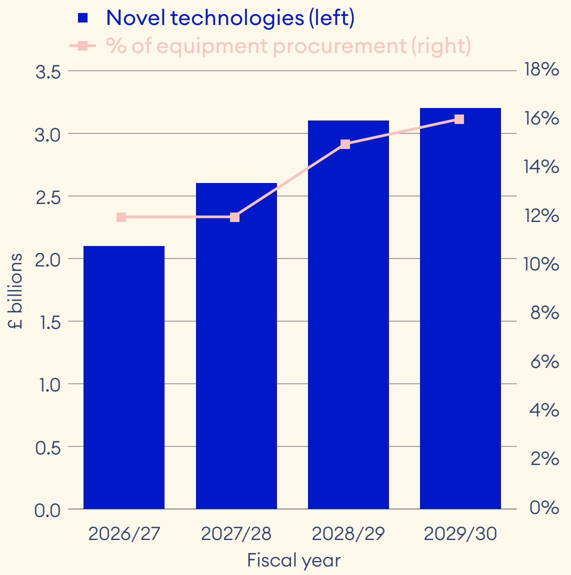
France's Thales can benefit from the growing demand for affordable air defence through ForceShield. It offers a cheaper means of countering drones and other low-flying threats than expensive interceptors.

The Iran and Ukraine wars have utterly changed procurement. Historically, a small number of expensive military assets have taken years to build. But increasingly, these advanced weapons systems are blended with affordable solutions delivered at scale and at speed – and speed has always mattered in warfare, by giving one side a technological edge.

The UK's Defence Investment Plan reflects this. It still prioritises naval nuclear deterrence and the Global Combat Air Programme, a stealth jet developed with Italy and Japan – both highly expensive undertakings. But there are no destroyers in it – heavily armed surface ships with a price tag to match. Like the Army and Royal Navy, the Royal Air Force is expected to move towards hybrid squadrons, in which swarms of uncrewed drones support pilots.

Figure 2.2: Funding the future

Novel technologies are set to account for a growing share of UK defence procurement.



Source: LSEG, Rathbones

What this means for investors

Heightened geopolitical tensions are prompting increases in defence spending. Various conflicts have depleted stocks of munitions, missile-guided seekers, and sensors. This requires years of restocking. The US' RTX is benefiting from efforts to restock and strengthen air and missile defences. It has leading positions in, for example, air-to-air missiles (the AMRAAM).

Agile defence-technology companies can develop disruptive solutions at speed. But established contractors also stand to gain if they can embrace innovation and combine it with their close ties to customers and deep understanding of combat missions. Start-ups and specialists are innovative. However, they often need to partner with major firms to scale production and manage the regulatory frameworks and compliance standards needed for government contracts.

Finding investment opportunities in drones is more challenging. First-person view drones, operated by people using cameras on the drones, have become commoditised: no company has a competitive edge. Ukraine alone produces eight million drones annually, across more than 100 manufacturers – and any easing of hostilities could flood the market, hitting margins. Supply of more sophisticated drones is dominated by large defence companies, but these account for only a small share of revenue.

The UK's BAE Systems, for example, has rapidly expanded its drone business, becoming one of the largest European producers outside Ukraine. Yet drones still account for only a single-digit proportion of group sales. US-listed specialist manufacturers such as AeroVironment are growing rapidly, although investors are already paying a premium for that growth.

In other words, the strongest investment potential doesn't, at the moment, lie in drones. But there are plenty of investment opportunities in both directing them and adapting to the revolution in warfare they have unleashed.

Cheap attacks, costly lessons
AI is reshaping cyber risk and corporate governance

Sonia Amrat-Nath, Stewardship Manager

It no longer takes a cyber Bond villain to cause corporate chaos. With cheap tools, a convincing email, and one exposed gap in the chain, attackers can now turn modest effort into expensive disruption.

Cyber risk is no longer just operational. It can stop sales, increase costs, squeeze margins, and damage trust in the companies we invest in. They can also draw the attention of regulators and unsettle investors if the financial hit looks material.

That is why companies need to protect not only data, intellectual property, financial assets, and reputation, but also the weaker links that can put them at risk. "You are the weakest link" was once Saturday-night theatre. For companies, it is now a useful way to approach cyber security. The better question for investors is whether management knows where the weakest links are, and whether the board is curious enough to question them before attackers do.

The bill for bargain breaches

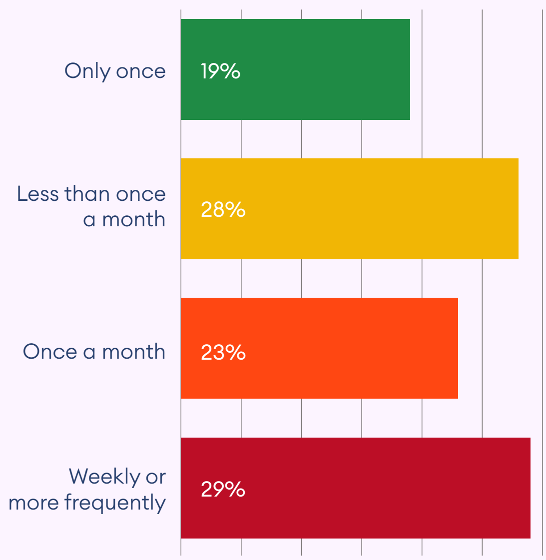
The hackers behind the cyber attacks on Marks & Spencer and Jaguar Land Rover in 2025 claimed to have stolen one billion customer records from these and other major companies. The attack on Jaguar Land Rover halted production and caused widespread delays across the company's supply chain. The Bank of England cited the incident as a key reason for lower-than-expected headline UK GDP growth in Q3 2025 and estimated its cost to the UK economy at close to £2bn. The US had its own costly example: a 2024 ransomware attack on UnitedHealth disrupted healthcare payments and cost around $3bn.

These incidents also show how cyber risk can cascade through the corporate supply chains and partner networks. A breach at a supplier, software provider or outsourced service partner can quickly become a listed company's operational, reputational and financial problem.

The threat of cyber attack is not new – the UK Government's 'Cyber Essentials' advice for companies is now 12 years old. Cisco's 2025 Cybersecurity Readiness Index found that 73% of UK organisations experienced a cyber incident in the past year. The global average cost of a data breach, including response and recovery, was estimated at about $4.4m according to IBM's Cost of a Data Breach report. The continued rise of AI technology in recent years is rapidly reshaping the cyber security landscape. These AI-related risks can be used to:

- Create convincing phishing emails that mimic colleagues, suppliers or IT teams.
- Target third-party partners with access to company data and systems.
- Use social engineering, such as phone calls or messages, to trick employees into approving payments or sharing access details.
- Scan public records, social media, cloud infrastructure, and company systems to find weak points faster, while AI coding tools and advanced large language models (LLMs) – such as Anthropic's Claude Mythos, built for cyber-security research – can help create low-cost, sophisticated attacks.
- Generate 'deepfake' voice or video impersonations to mimic senior executives or trusted contacts.

Figure 3.1: The breach club regulars
How often UK organisations have experienced cyber breaches or attacks in the past 12 months.



Source: UK Home Office, Rathbones

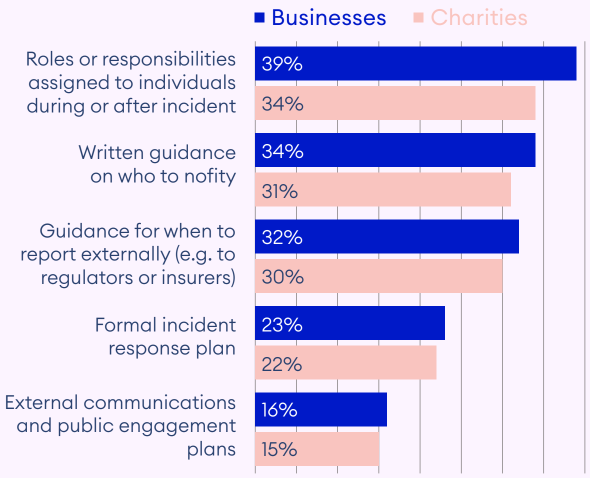
We believe small and medium enterprises are particularly vulnerable, due to often-constrained budgets and limited resources. AI is changing the economics of cyber crime, making attacks cheaper, faster, and more convincing. This gives criminals more opportunities to launch cyber attacks at scale, including targeting smaller companies that may have been deemed uneconomic to pursue in the past.

That matters for investors because the gap between cyber leaders and laggards may widen. Companies with resilient cyber defences may be better placed to protect long-term value.

Managing risk: defence needs directors
The increasing frequency, sophistication, and impact of cyber incidents underscore the importance of continually improving security measures. Companies can leave themselves vulnerable by underinvesting in cyber security. The UK Government's Cyber Security Breaches Survey 2025 suggests that board-level responsibility for cyber security has declined since 2021. The report stated that 38% of businesses had a board member with responsibility for cyber security in 2021, compared with 27% in 2025.

Nevertheless, our recent engagement with companies listed on Aim, the London Stock Exchange's market for smaller growth companies, in which we invest, has shown that good practices are being widely adopted. Most invest in cyber insurance, employee training, and board-level oversight of cyber incidents.

Figure 3.2: Ready on paper
Percentage of organisations* that have the following measures in place for dealing with cyber security breaches or attacks.



* 2,180 businesses and 1,081 charities
Source: UK Home Office, Rathbones

However, many of these companies don't use outside expertise to provide assurance over their practices or to conduct regular penetration testing (simulated attacks to test their defences). Although most firms monitor cyber risk and submit incident reports to boards, there is little evidence that board members receive training to provide rigorous oversight of cyber risk management practices. Only a small number of the companies we have engaged with have assigned cyber oversight to a specific board member. This is a concern for us, as we seek to protect the value of companies in our clients' portfolios, and we intend to keep this under review, engaging with companies where appropriate.

Directors need to know whether the company's defences work, whether external partners are being watched closely, and whether crisis plans would survive a real attack. This is not about signing off polished reports. It is about asking practical questions beforehand: have we tested the policies, do people know what to do, do critical partners know their role, and when the alarm sounds, who is in charge?

The attack on Marks & Spencer showed how cyber risk can enter through people and partners outside a company's own walls, after attackers reportedly persuaded third-party contractors to approve password resets. Weaknesses in suppliers or other third parties can quickly become a company's own problem. Strong governance, therefore, requires boards to look beyond internal controls and ask how critical partners assess, monitor, and respond to cyber threats.

Fighting code with code
While AI has lowered the costs and improved the efficiency of attacks, it can also strengthen defences. For example, AI can act as a force multiplier for cyber-security teams, helping companies spot unusual behaviour, monitor third-party risks, detect code flaws, prioritise fixes, recover affected systems, and contain threats before they spread. Companies that lead the pack will need to defend themselves against AI-enabled attacks while also harnessing AI as an opportunity.

Rising cyber threats should also support demand for businesses that help others defend themselves. The opportunity is not simply in the technology itself, but in how well companies use it.

The risks of failing to adapt as cyber criminals change their tactics are growing rapidly. We believe companies that adopt the highest standards of cyber security protection can represent a more attractive and robust investment. Companies that take cyber resilience seriously, through regular testing, AI-enabled defences and informed board oversight, may be better placed to protect long-term value. Those who continue to treat cyber security as an IT housekeeping matter may find the cost of complacency rising.

Snapshot
The global economy and markets

Figure of the month

60

The age at which one becomes a proper pianist, according to the great American player Ruth Slenczynska, who died in May aged 101. Professional pianists argue that life experience improves their playing over time. Older workers also pass knowledge to younger colleagues. Read our report and slideshow on the investment implications of an ageing world.

At a glance

57%
Fall in Ford's US electric vehicle sales (first half of 2026)

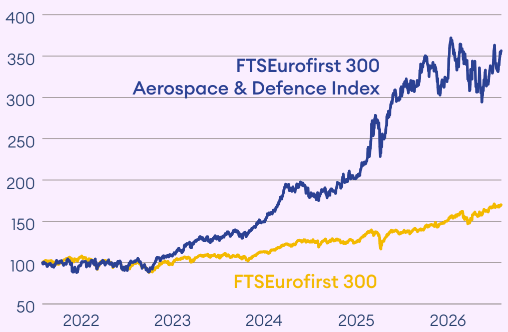
11%
Rise in global Lindt chocolate prices (first half of 2026)

47%
Share of UK electricity generated from renewables (past year)

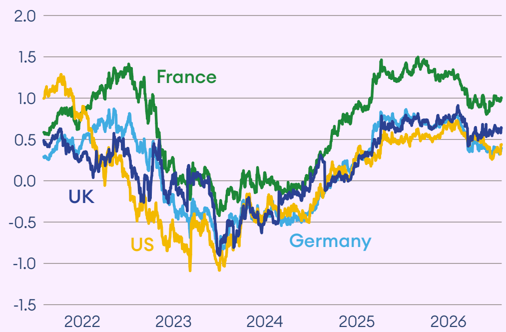
31%
Surge in European gas prices (June to July 2026)

Key market indicators

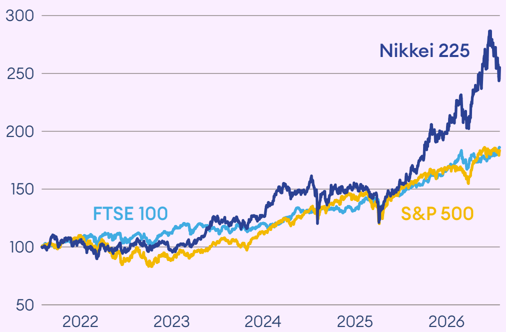
Equities
Total return in local currencies (1 August 2021 = 100)



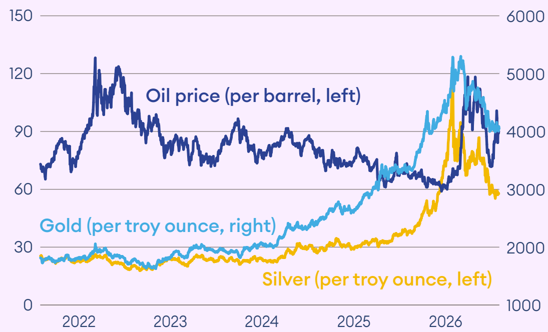
Government bonds
Difference between 2- and 10-year yields (%)



Equities
Total return in local currencies (1 August 2021 = 100)



Commodities
Oil, gold and silver prices in US dollars



Sources: FactSet, LSEG, Rathbones. Past performance is not a reliable indicator of future performance.

Find out more
Knowledge and insight

Alongside this monthly *Investment Insights* publication, we share a wide range of updates and analysis, from regular strategy commentary and video briefings to in-depth reports, all designed to help you understand what's driving the global economy, financial markets, and the outlook for investment returns. To explore more, visit www.rathbones.com/en-gb/wealth-management/knowledge-and-insight

---

Video updates
Stay informed with regular update videos from Robert Sears, our Chief Investment Officer, that explain how geopolitical tensions, market movements, and global economic trends could affect your portfolio.

Weekly and monthly digest
Keep up to date with regular insights from John Wyn-Evans, our Head of Market Analysis, as he explores the key themes shaping the global economy and investment environment.

Research reports and special updates
In line with our focus on long-term investing, we produce in-depth reports. These publications reflect the thinking behind our portfolio decisions and explore how structural trends, risks, and opportunities could affect investors over the long term. We also respond to big events with pieces that explain the implications for markets and your wealth.

Burnham is Prime Minister, Healey Chancellor. What does this mean for investors? We look at what the two new most powerful men in Britain might do for the economy and public finances in office – and what they should do.

The world is growing older. *The longevity economy* looks at the wider economic challenges, and the risks and opportunities in four sectors in which we invest: property, healthcare, must-have consumer goods, and nice-to-have consumer goods. Please also see our slideshow.

Experience and expertise
Rathbones has a large and experienced in-house research team covering global equities, fixed income, multi-asset strategies, and responsible investing. With specialists dedicated to analysing market trends, sectors, and individual securities, our team brings deep insight and rigorous discipline to every portfolio. This depth of knowledge allows us to uncover opportunities, manage risk effectively, and respond quickly to changing conditions, helping you to invest with greater confidence.

You can access this expertise in a range of ways, from fully bespoke discretionary portfolios to ready-made multi-asset funds, tax-efficient investment strategies, and specialist services for complex needs. To find out more and for details of your local office, visit www.rathbones.com/en-gb/wealth-management/contact-us