Creating Value with Cyber Security: What Leading PE Firms Are Getting Right

Private equity firms are beginning to treat cybersecurity less as a technical cost center and more as a strategic lever of portfolio value creation. Yet the gap between awareness and action remains wide. In Russell Reynolds Associates' Global Leadership Monitor, nearly a third of portfolio-company leaders list cyber risk among their top challenges, and almost as many admit they are not prepared to manage it [Figure 1]. Only 38% of PE organizations are proactively planning for technological change, even as most are introducing new digital and AI tools and products that expand their risk exposure.

We recently sat down with many senior cyber operating partners and cyber security executives in private equity firms, and our interviews reveal why progress is uneven. Many firms still handle cyber as a compliance exercise — a checklist of controls and annual assessments — rather than a dimension of investment governance. Others have started embedding cyber leaders at every stage of the investment lifecycle — evaluating risk exposure during due diligence, aligning remediation efforts with value-creation plans, and protecting enterprise value ahead of exit.

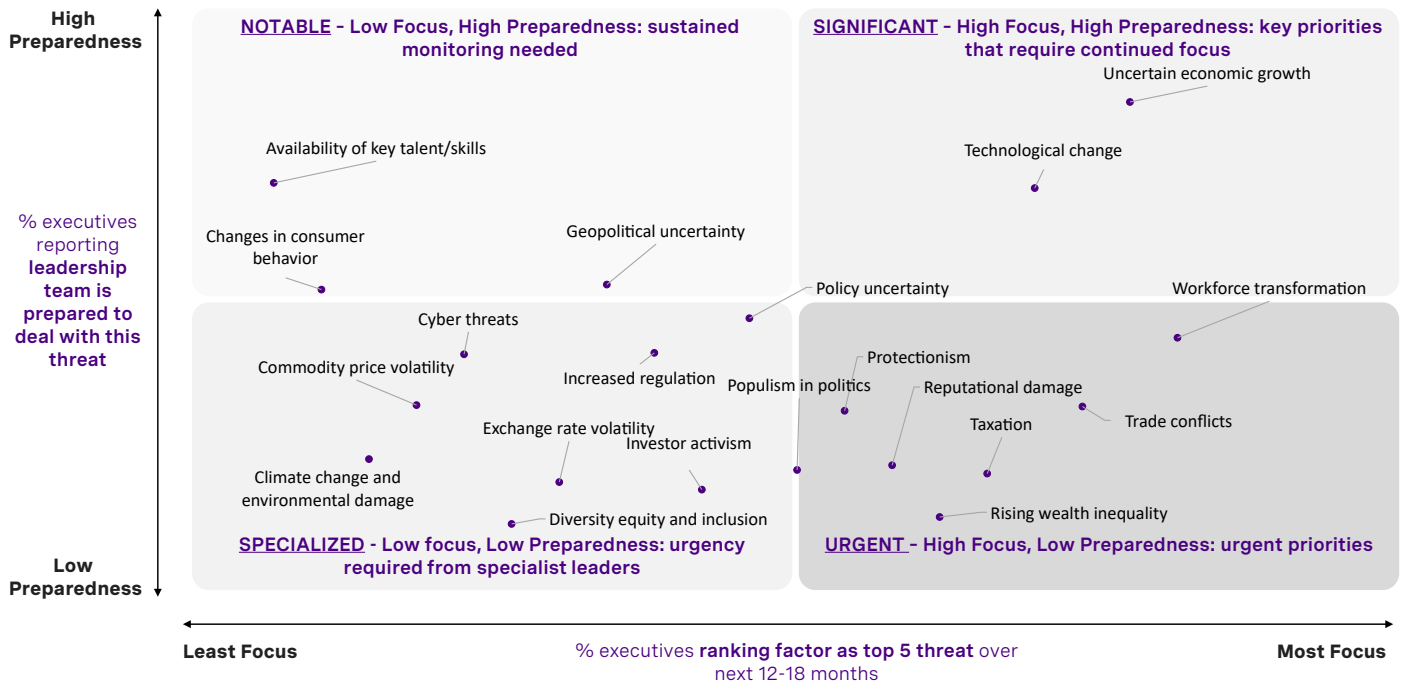
These leaders describe a structural shift. Value protection is becoming inseparable from value creation. A single breach can erode returns, yet firms that can measure, benchmark and scale resilience across their portfolios are starting to treat cyber maturity as a competitive differentiator.

72%

of private equity firms across the US and Europe reported a serious cyber incident at one of their portfolio companies in the past three years, with an average cost of $3.4 million per incident.

2025 S-RM Cyber Incident Insights Report

Figure 1: Executive Perceptions of Global Threats: Focus vs. Preparedness



Source: Russell Reynolds Associates Global Leadership Monitor H1 2025

The following sections examine how approaches to cyber in private equity are diverging: where the most mature firms are investing, where cultural and governance gaps persist, and how the next wave of AI-driven change will test every portfolio's resilience.

01 | The state of cyber in private equity: awareness without readiness

Cybersecurity has climbed up the private-equity agenda, but most firms are still treating it as a hygiene issue rather than a core element of investment governance. Boards have started to ask questions; they are not yet asking the right ones. One operating partner described a familiar pattern: Boards are "focused on spend and peer benchmarking rather than risk appetite, incident readiness, or control effectiveness."

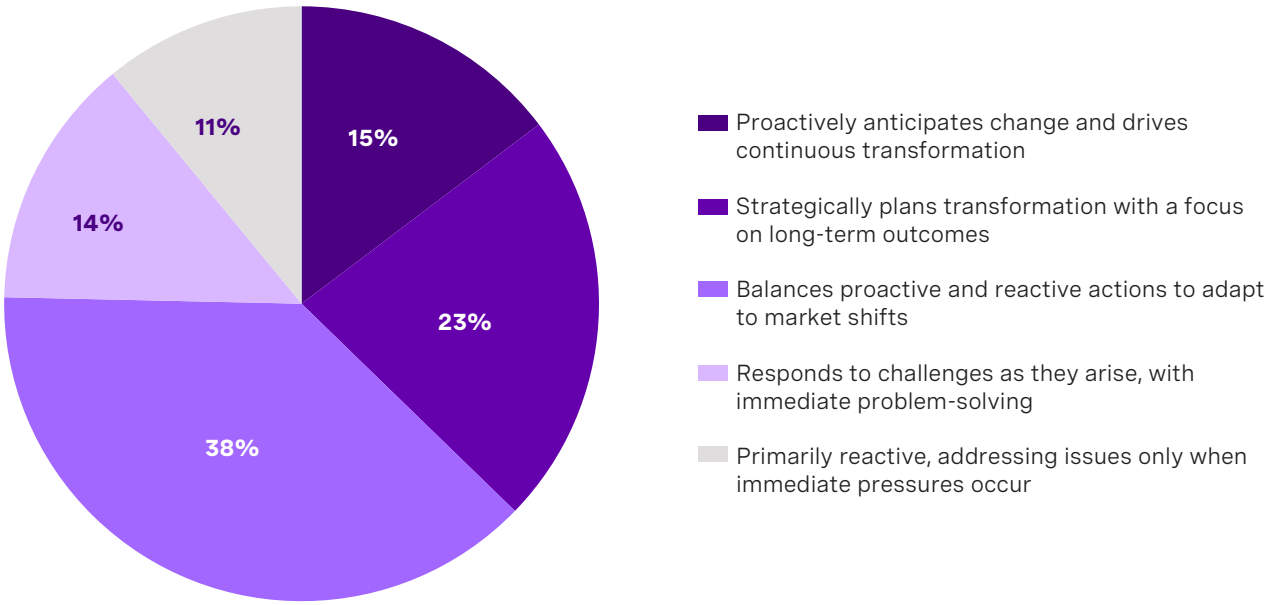
This lack of readiness stems less from ignorance than from structure. Cyber accountability is often fragmented between operating partners, portfolio company management teams, and external advisors.

> "Boards have become more tactical in their questions — they ask if MFA (Multifactor Authentication) is rolled out everywhere rather than strategy or risk appetite."

Meanwhile, the operating environment is shifting faster than most firms can adapt. Only 38 percent of PE organizations are proactively planning for technological transformation [Figure 2], even though most have introduced cloud-based applications and data pipelines in the past year that expand their attack surfaces [Figure 3]. Innovation has outpaced protection.

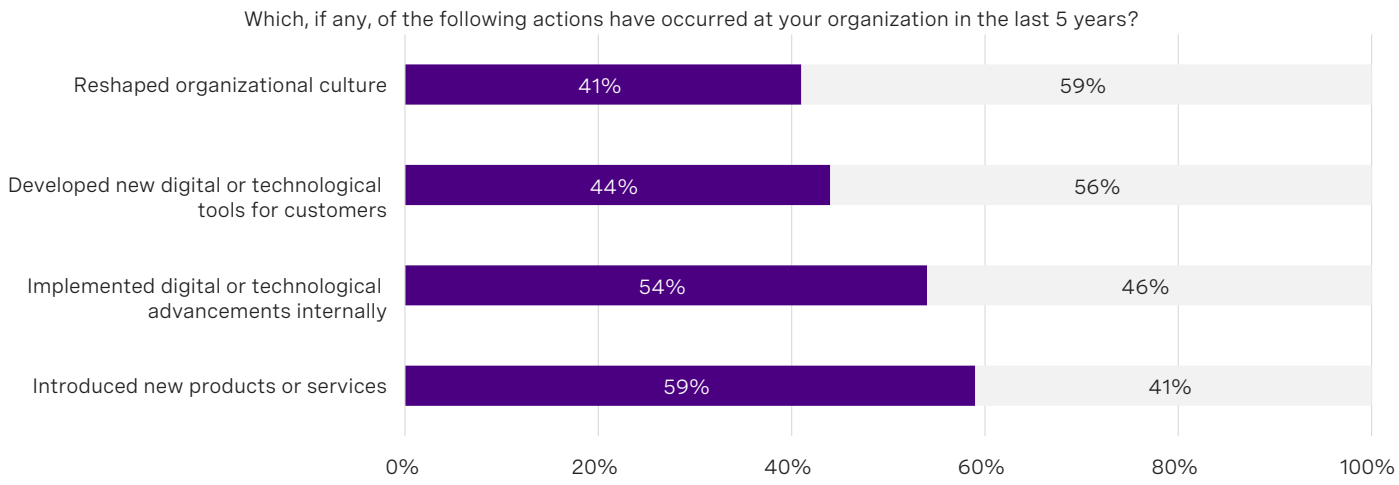
Figure 2: PE Approach to Transformation

How would you describe your organization's approach to transformation?



Source: Russell Reynolds Associates Global Leadership Monitor H1 2025

Figure 3: Organization Changes at PE Firms in the Last 5 Years



Source: Russell Reynolds Associates Global Leadership Monitor H1 2025

The firms furthest ahead are those treating cyber as an investment discipline rather than a technical control set. They use continuous control validation, zero-trust architectures, and portfolio-level cyber maturity dashboards to inform decisions. Others still rely on reactive incident response rather than predictive threat modeling. For these investors, cyber remains an afterthought until an incident or investor query forces attention.

> "Most firms find religion through pain."

The sector is therefore divided not by budget but by mindset. A minority of firms are beginning to institutionalize resilience; the rest are still reacting to events. As one cyber operating partner observed, "value protection is inseparable from value creation — but most firms still run them on separate tracks."

02 | Embedding cyber across the investment lifecycle

For many private-equity firms, cybersecurity still begins after the deal closes. The most effective firms start much earlier. They embed cyber expertise across the investment lifecycle — assessing inherited risks during diligence, integrating remediation into the value-creation plan, and protecting valuation at exit.

Due diligence.

Cyber diligence has moved from box-ticking to risk pricing. During due diligence, leading investors perform actions such as penetration testing, cloud configuration audits, and identity access management (IAM) reviews to identify inherited risk. Several interviewees said that while cyber rarely derails a deal, it increasingly shapes valuation and day-one priorities: "You're usually buying companies with some inherent issues — you build that cyber risk into the price."

Value-creation phase.

> "You can't manage what you can't measure."

Once a company joins the PE portfolio, attention often shifts back to margin expansion or growth demands. The strongest firms implement cyber remediation roadmaps aligned to their value-creation plans. These often include endpoint detection and response (EDR) systems, data loss prevention (DLP) policies, and supply chain risk scoring. Firms that measure mean time to detect (MTTD) and mean time to respond (MTTR) across portfolio companies achieve materially higher operational resilience. One operating partner put it simply: "You need someone who can connect the dots across the portfolio, measure, and tell if they're investing enough in cyber."

Others described using cross-portfolio benchmarking metrics or common dashboards to track security maturity. These measures turn resilience into something quantifiable — and investable.

Exits and value protection.

As exits approach, attention shifts to investor assurance. Firms conduct red-team exercises, ransomware kill-chain simulations, and compliance attestations against ISO 27001, SOC 2, and NIST CSF frameworks to prove readiness to potential buyers. A cyber breach in the final months of an investment holding period can derail a transaction by wiping millions in valuation overnight and eroding buyer confidence.

Cyber teams therefore must shift from tactical development to investor assurance: validating controls, auditing third-party dependencies, and documenting compliance with industry regulatory standards; "There's nothing worse than when a portfolio company has a breach — because PEs care about valuation, and a breach lowers that valuation."

For leading firms, this is now standard practice. One cyber executive described their role as "protecting valuation at the moment it matters most."

03 | Divergent operating models: from reactive to institutionalized

Across private equity, two contrasting models of cyber management are taking shape. Most firms still run on a reactive model: fragmented accountability, over-reliance on external consultants, and limited visibility across the portfolio; while others have created a more institutionalized model: one that benchmarks, measures and implements resilience at scale.

In the reactive model, security remains an operational cost. Deal teams shirk responsibility to portfolio company management, which then outsources security and risk assessments to large consultancies. The result is a patchwork of reports and recommendations few companies can execute. One interviewee said the Big Four's playbooks "can overwhelm management teams and fail to align with the realities of mid-market portfolios." External advice from these players doesn't always add up to a coherent strategy.

> "Outputs offered by the Big Four aren't always well drafted to help you make strategic decisions."

Reactive firms focus on control checklists and audit cycles, but rarely connect cyber posture to investment decisions. Maturity measurement remains inconsistent, and lessons from a breach at one portfolio company rarely cascade effectively across the portfolio.

By contrast, institutionalized models treat cyber as an operating discipline. Leading cyber operating partners have data pipelines from every portfolio company, common reporting formats, and direct access to key stakeholders. Several described dashboards that quantify risks, influence adoption, and recovery times in real time: "Because we're data-driven, we can show where each company stands — and even predict the likelihood of an incident."

These firms view scale as their differentiator: one cyber operating partner oversees 40 to 50 companies in their portfolio, using standardised metrics and shared tooling rather than bespoke one-off fixes. They host regular CISO forums, publish playbooks, and embed cyber in investment theses from acquisition to exit. As one interviewee stated: "We're the only function that speaks to every portfolio company — that's a privileged position."

The difference is visible in outcomes. Institutionalised models report fewer incidents, faster response times, and higher confidence from investors. For others, progress still depends on the next crisis: "The gap isn't budget — it's mindset."

04 | Leadership and governance: turning compliance into conviction

The strongest cyber programs in private equity are built less by technology but more through leadership alignment. Most leaders now acknowledge cyber as a board-level issue, but few engage with it meaningfully as part of investment governance. One operating partner said bluntly: "Rarely is there a board member who can really engage on cyber."

This narrow focus misses the wider organizational question: who owns cyber risk? In many firms, accountability diffuses across operating partners, CISOs and PortCo management teams, with no clear governance mechanisms in place. The result is compliance activity without conviction.

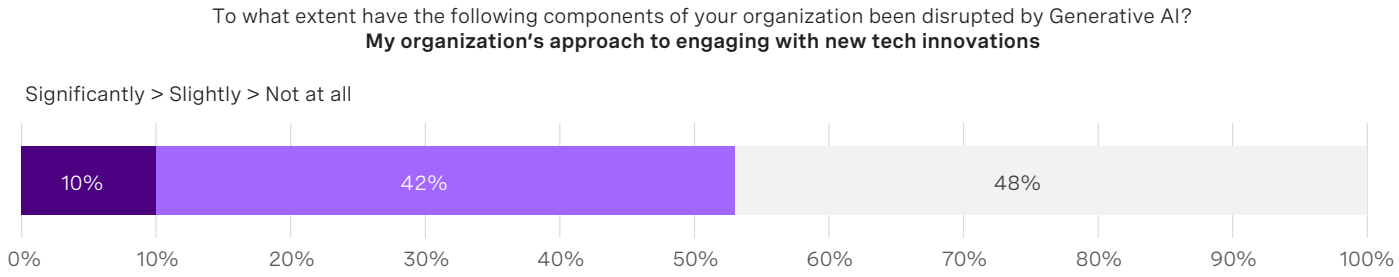
Leading firms treat cyber resilience as a leadership competency. They tie executive compensation to measurable improvements in NIST-aligned maturity, normalize peer learning through CISO roundtables, and leverage threat intelligence briefings to educate investment professionals. One interviewee described success as "winning the hearts and minds of investment professionals and portfolio leaders — that we're in this together."

Another added a caution: "Don't manage by checklist. You'll end up with order takers, not leaders." Effective cyber governance integrates metrics into board reporting: control effectiveness scores, regulatory compliance heatmaps, and readiness indices. In these firms, compliance evolves into culture and conviction.

05 | The next inflection point: AI and emerging risks

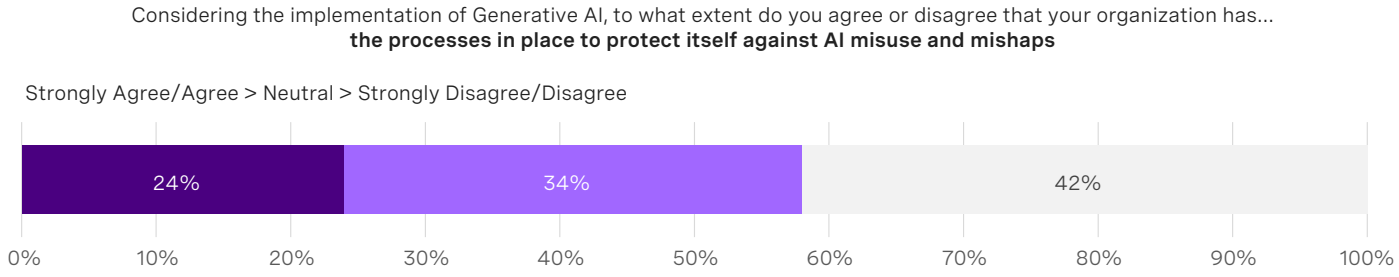
Artificial intelligence has become the newest fault line in portfolio resilience. Half of all leaders surveyed say AI has already changed how they approach innovation, yet 52% expect its adoption to disrupt existing cyber-safeguards [Figure 4]. More than half worry that AI could inadvertently weaken their core internal processes [Figure 5].

Figure 4: Generative AI Disruption on PE Innovation



Source: Russell Reynolds Associates Global Leadership Monitor H1 2025

Figure 5: PE Concern Around AI Compromise on Internal Processes

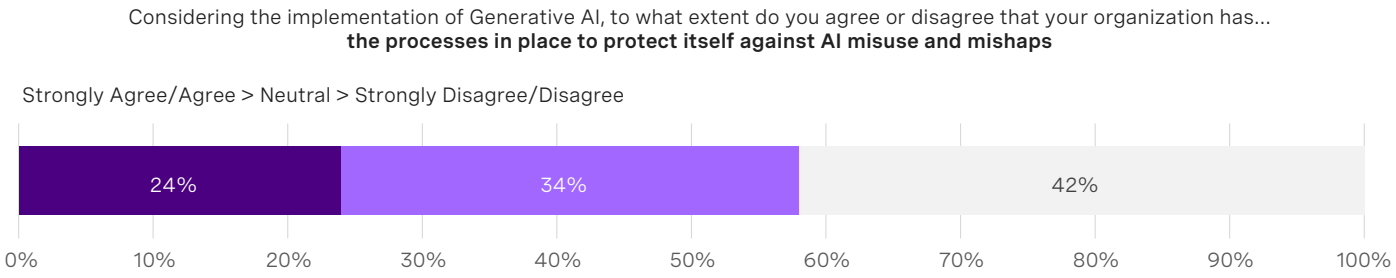


Our interviews with cyber leaders in PE suggest that these fears are well-founded. Several cyber leaders described AI as a democratizing force — one that empowers both attackers and untrained users inside the firm. Attackers are already using generative AI tools to accelerate phishing, deepfakes and even automated ransomware payment negotiations. "What used to take sixty days now happens in hours," said one interviewee, "Attackers innovate in hours, not months".

> "AI is the first big shift where anyone can use it — it empowers non-technical people. That changes the whole risk model."

The defensive opportunity is just as real. Leading firms are experimenting with AI-driven threat detection, vulnerability scanning and application testing to close the speed gap. Yet, more than half of survey respondents from PE-backed companies felt that their organizations had sufficient processes in place to protect itself against AI negligence [Figure 6]. Success depends less on tools than on governance. One cyber executive warned: "If you start with a department of 'no', the organization rejects it."

Figure 6: PE Protection Against AI Misuse and Mishaps



Source: Russell Reynolds Associates Global Leadership Monitor H1 2025

AI is forcing PE firms to revisit the fundamentals of oversight — deciding who can deploy it, how its outputs are monitored, and when innovation becomes risk exposure. Much like the shift to the cloud several years ago, private equity firms and their portfolio companies must invest the time to understand AI. Just as cloud adoption required leaders to grasp its fundamentals, cybersecurity in an AI-driven world demands that executives at least understand the language of AI, even if they aren't technical experts. Without that foundation, it becomes nearly impossible to anticipate or defend against the emerging threats introduced by AI.

> "If you don't know what AI is doing in the world, how can you even begin to imagine the threats it creates or how to defend against them?"

06 | What leading firms do differently

The most mature private-equity firms are no longer debating whether to invest in cyber, but how to make that investment scale. Across interviews, five consistent practices emerged.

Integrate cyber into the deal lifecycle

Cyber assessments now shape valuations and remediation planning from the outset.
"Every investment memo now includes a statement on cyber posture — pre-deal and post-close."

Institutionalize measurement and benchmarking

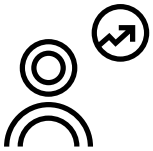
Leaders track maturity across portfolios through shared dashboards and external benchmarks, turning resilience into something visible and comparable.
"Show them they're in the bottom quartile — that's when they listen."

Build scalable operating models

High-performing firms use repeatable playbooks and shared systems rather than one-off fixes.
"We had to build a program that scales across 200+ portfolio companies — systems, data, and relationships."

Foster peer learning and community

CISO forums and cross-portfolio exchanges accelerate progress by sharing insights on what works.
"Bringing CISOs together and letting the most mature leaders present their work — that's the best peer learning you can get."



Align incentives with outcomes

Several firms are tying management rewards to measurable improvements in cyber maturity: as one interviewee said, "The firms that connect cyber results to leadership incentives see culture change fastest."
These approaches share one principle: scale comes from systems and governance, not from heroic firefighting.

07 | The leadership mindset shift

Progress in cyber is no longer defined by tools or spend, but by mindset. The firms outpacing their competition treat security as a leadership discipline — measurable, repeatable, and shared. They understand that culture, not compliance, determines how a company views security and how effectively they respond under pressure during, at times inevitable, cyber events.

> "Cyber resilience starts as a control problem but ends as a leadership one."

One cyber operating partner put it plainly: "You're not the smartest person in the universe. You don't know what's best all the time." That humility — combined with persistence and data — distinguishes the firms turning cyber from a technical concern into a source of trust, resilience and operational strength.

Another CISO noted, "Everyone accepts that breaches will happen, but when they do, people are surprised by how incompetent or negligent they appear. It's rare for a breach to be truly unavoidable. Setting the right expectation — that it will be an embarrassing experience — is one of the hardest things to prepare people for."

Conclusion

As cyber risk becomes inseparable from value creation, private equity firms can no longer rely on frameworks or vendors alone — they must cultivate a cyber governance culture and empower the right leaders. Building resilience at scale depends on embedding cyber mindset into investment governance, rewarding transparency, and ensuring every portfolio company has champions who translate risk into action. The firms that will lead the competition in the next decade are those that ensure security is a shared leadership language across investment partners, operating partners, and portfolio company board and management teams.

At Russell Reynolds Associates, we see this shift firsthand. Progress begins not with technology, but with people and culture — with leaders who model curiosity, humility, and conviction around resilience and innovation. Helping firms identify, assess, and develop these leaders is where we believe lasting competitive advantage begins.

Authors

Angela Jung co-leads Russell Reynolds Associates' Cybersecurity practice and is a member of Russell Reynolds Associates' Technology practice globally. She is based in New York.

Ahmed Jamil co-leads Russell Reynolds Associates' Cybersecurity practice and is a member of Russell Reynolds Associates' Technology practice globally. He is based in Chicago.

Harriet Wood co-leads Russell Reynolds Associates' Cybersecurity practice and is a member of Russell Reynolds Associates' Technology practice globally. She is based in London.

George Head leads commercial strategy and insights for Russell Reynolds Associates' Technology sector. He is based in London.

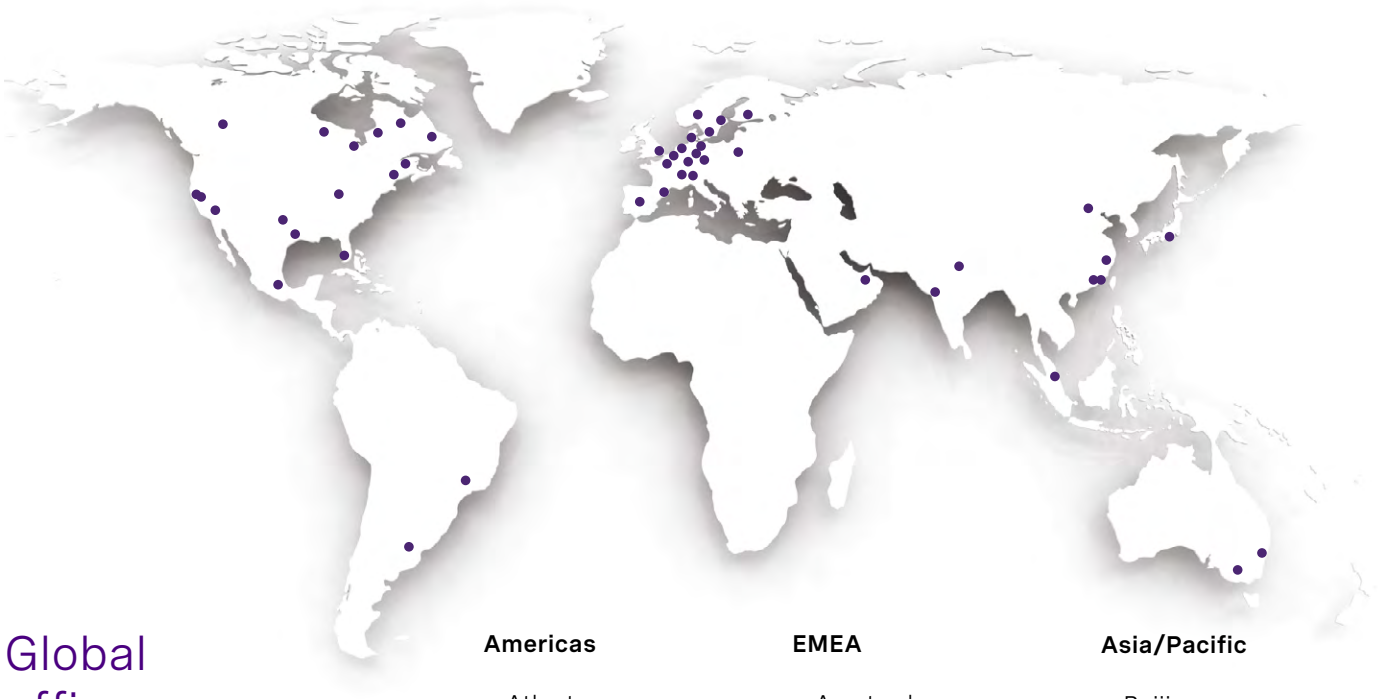
Robert Alexander is a member of the commercial strategy and insights for Russell Reynolds Associates' Technology sector. He is based in New York.

Camille Golub is an intern for Russell Reynolds Associates' Technology sector. She is based in New York.

About Russell Reynolds Associates

Russell Reynolds Associates is a global leadership advisory firm. Our 500+ consultants in 47 offices work with public, private, and nonprofit organizations across all industries and regions. We help our clients build teams of transformational leaders who can meet today's challenges and anticipate the digital, economic, sustainability, and political trends that are reshaping the global business environment. From helping boards with their structure, culture, and effectiveness to identifying, assessing and defining the best leadership for organizations, our teams bring their decades of expertise to help clients address their most complex leadership issues. We exist to improve the way the world is led

www.russellreynolds.com



Global offices

Americas

- Atlanta
- Boston
- Buenos Aires
- Calgary
- Chicago
- Dallas
- Houston
- Los Angeles
- Mexico City
- Miami
- Minneapolis/St.Paul
- Montreal
- New York
- Palo Alto
- San Francisco
- São Paulo
- Stamford
- Toronto
- Washington, D.C.

EMEA

- Amsterdam
- Barcelona
- Berlin
- Brussels
- Copenhagen
- Dubai
- Frankfurt
- Hamburg
- Helsinki
- London
- Madrid
- Milan
- Munich
- Oslo
- Paris
- Stockholm
- Warsaw
- Zürich

Asia/Pacific

- Beijing
- Hong Kong
- Melbourne
- Mumbai
- New Delhi
- Shanghai
- Shenzhen
- Singapore
- Sydney
- Tokyo