EXECUTIVE PERSPECTIVES ON TOP RISKS AND OPPORTUNITIES

for the Near - and Long - Term

protiviti®
Global Business Consulting

Navigating disruption, modernisation and mission resilience

Preparing for a decade shaped by security, emerging technology and geopolitical volatility.

For aerospace and defence leaders, risks rarely emerge in isolation. Technology disruption, regulatory uncertainty, geopolitical instability, supply chain constraints, ageing infrastructure and workforce challenges increasingly converge, testing organisations' ability to modernise, protect sensitive assets and deliver on mission-critical commitments.

That convergence makes response more difficult. Leaders can plan for many transformation and protection needs, but response often requires confronting "unknown unknowns" — sudden policy shifts, geopolitical events, trade restrictions or emerging threats — in an industry shaped by long programme cycles, intensive regulation, exacting technical requirements and major capital commitments.

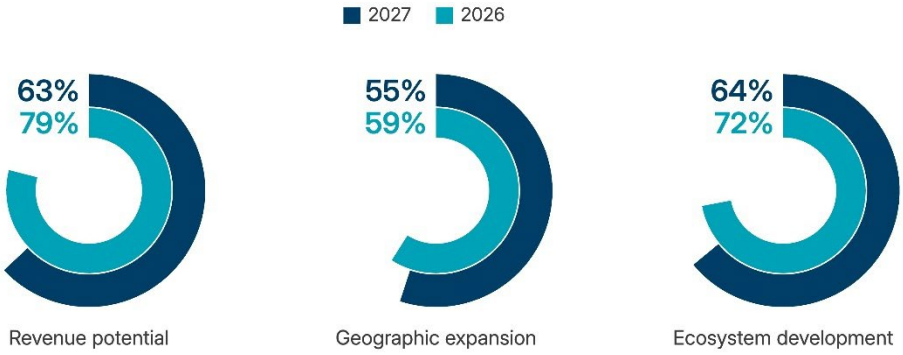
This year's Top Risks and Opportunities Survey reflects that readiness challenge. Disruptive innovation, regulatory change, technology skills, legacy infrastructure and geopolitical instability lead the near-term risk outlook. Cybersecurity and infrastructure modernisation top planned investments, while security and privacy, AI, geopolitics, and supply chain and third-party ecosystems dominate the 10-year view.

Together, the findings point to an industry that must modernise without sacrificing resilience. Leaders must connect cybersecurity, infrastructure, data, AI, workforce and supply chain decisions rather than treat them as separate initiatives. Those that turn innovation into operational capacity, strengthen their ecosystems and prepare for unpredictable disruption will be best positioned for the decade ahead.

Where do A&D leaders see the greatest opportunities for their organisation over the next two to three years?

For aerospace and defence leaders, growth remains firmly in view, but expectations are more measured than they were a year ago. Nearly two-thirds of respondents see opportunities in ecosystem development (64%) and revenue growth (63%), while 55% anticipate opportunities through geographic expansion. Agreement declined across all three areas compared with the prior year, suggesting not an absence of demand, but greater selectivity about where growth will occur and which organisations are positioned to capture it.

Views on opportunities for growth



Based on a five-point scale assessing agreement/disagreement.
Percentages reflect the sum of "Agree completely" and "Agree somewhat" responses.

Growth prospects remain strong as defence spending rises, depleted inventories are replenished and investment accelerates in areas such as autonomous systems, quantum technologies and post-quantum security. However, opportunities will vary widely depending on where organisations sit within the defence ecosystem and how closely their capabilities align with shifting spending priorities.

Revenue growth is likely to favour organisations positioned around emerging technologies, modernisation initiatives and mission-critical capabilities. Those tied to ageing platforms or lower-priority programmes may face a more limited outlook despite broader market expansion.

Ecosystem development ranks as the sector's leading opportunity, highlighting the value of partnerships in accelerating innovation, expanding capacity and accessing specialised expertise. Geographic expansion also presents growth potential through exports, licensing arrangements and local production models, though success will depend on navigating export controls, regulatory requirements, trade policy and geopolitical uncertainty.

Taken together, the findings point to an A&D market with significant opportunity but no single path to growth. Organisations that align their portfolios with evolving mission priorities, build high-performing ecosystems and adapt quickly to changing demand will be best positioned to capture growth and strengthen their competitive advantage.

What priorities do leaders see as most important to maximising the value of AI deployments?

For aerospace and defence organisations, the AI conversation is shifting from experimentation to execution. Leaders prioritise workforce readiness (48%), integration with existing technologies, processes and people (43%), stronger governance and accountability (35%), and protection of sensitive data used to train and operate models (31%). The emphasis is not on deploying AI faster but on creating the conditions for reliable operational and mission value.

48%

rank better equipping the workforce to realise AI's value proposition as a top priority.

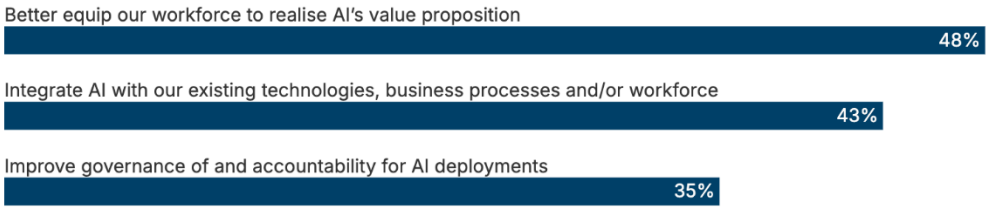
Workforce enablement leads for good reason. AI can expand capacity in a sector facing retirements and scarce technical talent, but employees must know how to use it and trust its role in their work. The goal is to augment people, enabling a fixed or shrinking workforce to increase output, improve decisions and complete work that might otherwise go undone. That requires role-specific training, practical use cases and clear expectations for human judgement.

Integration is equally critical. A&D companies often operate complex engineering environments, long-running programmes, acquired systems and legacy infrastructure. AI isolated from those environments will not deliver value at scale. Leaders need to embed it in workflows spanning digital engineering, finance, human resources and programme operations while strengthening the data and technology foundations beneath them. The results may also understate the sector's maturity: companies can be cautious about back-office AI even as AI embedded in defence and space

products is more advanced, and classified applications cannot be discussed openly.

Governance and data security must bridge those worlds. A&D organisations handle classified information, controlled technical data, intellectual property and sensitive supply chain information. Clear accountability, approved-use policies, model oversight and disciplined data controls are essential to innovate without creating unacceptable security, compliance or mission risk. The organisations most likely to realise lasting AI value will connect the technology to real work, prepare employees to use it and govern it according to mission sensitivity.

Top AI opportunities – A&D Leaders



We asked A&D leaders three specific questions about their views on the organisations' ability to (1) transform the enterprise, (2) protect enterprise value, and (3) respond with agility to market opportunities and risks. What did they tell us?

A&D leaders are more confident manageing planned change than responding to sudden disruption. A majority report high or very high confidence in their ability to transform the enterprise (53%) and protect enterprise value (51%). Confidence in responding with agility falls to 45%, while 46% rate it moderate. The gap reflects an industry that can plan around known requirements but cannot easily pivot when government priorities, regulations, conflicts or trade conditions change.

Transformation is especially demanding for large contractors. Long-duration programmes, extensive property, plant and equipment, complex approval structures and heavy regulatory obligations can slow modernisation. Smaller, engineering-led companies may move faster, while larger



organisations often acquire innovation — then risk constraining it through integration and established processes. Even so, transformation remains largely within management's control: Leaders can set roadmaps, allocate capital and execute against known objectives. Protection follows a different A&D pattern. Scale, diversified programmes and deeper resources can help major contractors secure sensitive assets and absorb disruption. Smaller companies may be more agile but more exposed to the loss of a core programme, a change in technical standards or a setback affecting a narrow portfolio. Both transformation and protection can address known conditions and "known unknowns," even when execution is difficult.

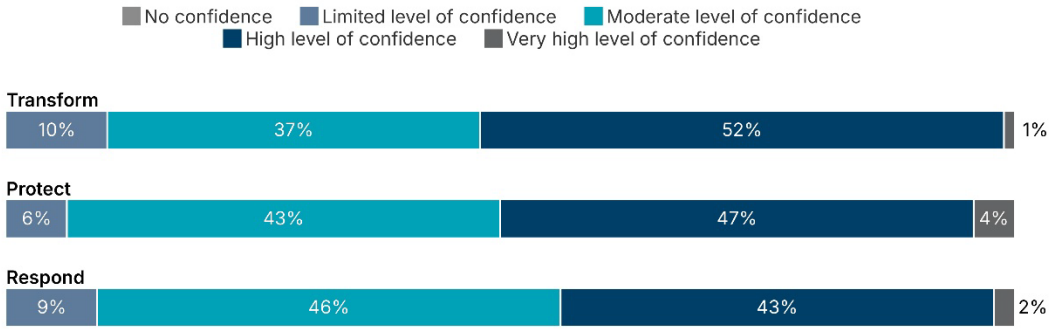
Responding is harder because A&D organisations must contend with "unknown unknowns": an unforeseen government action, regulatory reversal, geopolitical event, trade restriction or emerging threat. Long programme cycles, exacting specifications, restricted supply chains and major up-front investments limit how quickly companies can redirect production, redesign systems or replace suppliers — even when mission needs shift rapidly.

The implication is not that the sector lacks resilience, but that traditional resilience planning has limits. Building greater response confidence will require visibility across programmes and lower-tier suppliers, faster decision rights, scenario planning and crisis governance tied to operational and mission consequences. In A&D, agility is less about moving quickly in every circumstance than recognizing change early enough to act before technical, contractual and supply chain commitments narrow the available options.

53%

report high or very high confidence in their organisation's ability to transform the enterprise.

Views about the ability to transform, protect and respond – A&D leaders



What are the most significant near-term concerns and risks on the minds of A&D leaders?

The common thread in this year's rankings is readiness for disruption. A&D leaders are confronting interconnected risks: Technology can alter mission requirements, regulation can reshape investment decisions, workforce gaps can slow modernisation, and geopolitical shifts can constrain supply. The results describe a connected risk system rather than isolated concerns.

Top five near-term risks – A&D leaders

AD

Question	2027	2026
Emergence of new risks from implementing artificial intelligence	3.80	3.09
Cyber threats	3.66	3.90
Rapid speed of disruptive innovations enabled by emerging technologies and/or other market forces	3.66	2.90
Heightened regulatory change, uncertainty and fragmentation	3.56	3.02
Limited access to workforce skills needed to adopt new and emerging technologies	3.50	3.02

Disruptive innovation leads the near-term outlook at 3.66, up from 2.90 last year. The increase links primarily to AI and rapid changes in warfare, including drone proliferation and the unfavourable economics of countering low-cost threats with expensive defensive systems; quantum computing is emerging at the margins. In A&D, innovation risk can quickly affect programme priorities, platform relevance and defence economics.

Regulatory change ranks second at 3.56, followed by limited access to technology skills at 3.50. Rules introduced through policy or executive action may not endure, complicating the timing and scale of compliance investments. Meanwhile, retirements, scarce technical talent and resistance to changing established processes can limit adoption of the technologies needed to compete and deliver.

Legacy infrastructure and geopolitical instability, tied at 3.49, reinforce the readiness challenge. Acquired systems, technical debt and ageing platforms can impede modernisation, while shifting alliances, conflicts, tariffs and trade policies can restrict sourcing. Because A&D companies cannot freely substitute suppliers or jurisdictions, policy changes can quickly create production, maintenance and mission consequences.



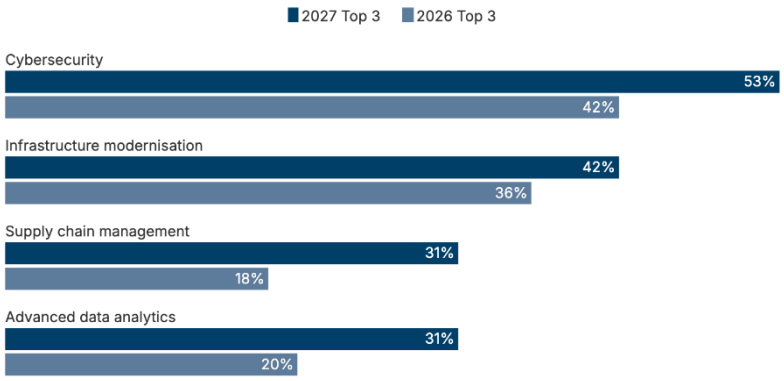
Cybersecurity is embedded across the rankings rather than absent. Privacy and identity compliance, third-party exposure, emerging technology and supply chain uncertainty all carry cyber implications. Cybersecurity likely would have ranked near the top if listed separately — a view reinforced by its position as the survey's leading investment priority.

The bottom line: No single risk defines the outlook. A&D leaders must manage the convergence of technology, policy, talent, infrastructure, cybersecurity and geopolitics. That requires treating risk as a portfolio and strengthening the workforce, systems, suppliers and decision-making capabilities that support operational and mission resilience.

Given these near-term risk issues, where do organisations plan to invest most?

A&D organisations are investing in the foundations of secure modernisation and operational continuity. Cybersecurity leads at 53%, followed by infrastructure modernisation at 42%. Supply chain management and advanced data analytics, both at 31%, complete the top tier. Together, these priorities signal a focus on protecting sensitive assets, sustaining operations and improving decisions.

Top strategic investment priorities – A&D market



Cybersecurity rose from 42% last year, reinforcing that cyber risk cuts across privacy, identity, emerging technology, third parties and supply chains. A&D executives often define cybersecurity broadly to include hacking, espionage, data theft and intellectual property loss. In a sector built on sensitive information and complex supplier networks, cyber investment is a continuing response to evolving threats.

53%

rank cybersecurity as a top strategic investment priority.

Infrastructure modernisation is integral to that effort. Advanced security is difficult to deploy on ageing platforms, and many A&D companies carry technical debt from acquisitions, disparate systems and delayed ERP upgrades. Modernisation creates the foundation for stronger security, more effective use of data and the integration of emerging technologies.

Supply chain management and advanced analytics support the same readiness agenda. Supply chain investment can strengthen visibility, regulatory flow-down and supplier compliance in an industry with constrained sourcing options. Analytics can help leaders identify emerging issues, improve productivity and extract greater value from programme and business data. Data privacy, meanwhile, fell from 48% to 29%, possibly indicating that foundational capabilities are established or increasingly embedded in broader cyber and compliance programmes.

Workforce skilling remains a potential blind spot. Access to technology skills ranks among the leading near-term risks, yet human capital management and workforce skilling received only 20% of top-three selections. AI and automation can help a fixed or shrinking workforce increase output, but only if organisations equip employees to use those tools effectively.

Taken together, the results point to an integrated investment agenda. A&D resilience increasingly depends on modern infrastructure, robust cybersecurity, transparent supply chains, trusted data and a workforce prepared to translate those capabilities into operational and mission value.

How do A&D leaders view the 10-year risk outlook for their organisation?

Over a 10-year horizon, A&D leaders are focused on forces that could reshape mission capability, platform relevance and the defence industrial base. Security and privacy remain the most frequently selected theme at 53%, followed by AI deployments at 46%. Geopolitical challenges rose to 37%, while supply chains and third-party ecosystems reached 33%. The strategic imperative is to preserve mission assurance as technology, policy and global relationships evolve.

Security remains the anchor risk despite declining from 58% last year. David Brand cautions against overinterpreting the shift: Respondents may be assigning more of their top-three selections to AI and geopolitics, which increasingly overlap with security. Cyber threats can compromise classified



data, erode intellectual property, disrupt production and affect mission systems. Security is therefore a permanent operating requirement.

AI's rise from 41% to 46% reflects its growing influence on weapon systems, space capabilities, engineering, production and the workforce. Over the next decade, AI could change how platforms are designed, operated and defended — and determine which programmes remain relevant. Realising its value will require integration into mission environments without compromising data security, human oversight or trust.

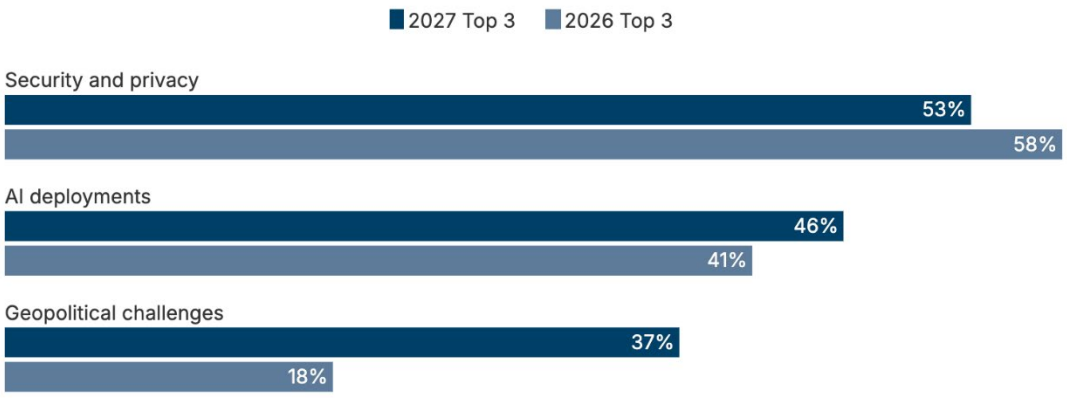
Geopolitics and supply chain ecosystems carry equally direct consequences. Conflicts, shifting alliances, export controls, tariffs and industrial policy can determine where companies source components, manufacture systems and sell capabilities. Because defence programmes depend on qualified suppliers, approved jurisdictions and long production cycles, disruption can affect capacity, delivery, sustainment and military readiness.

Quantum computing remains lower in the rankings at 12%. Although its selection rate has tripled from 4%, it remains underrecognized rather than unimportant. That distinction matters in A&D, where sensitive information and fielded systems may require protection for decades, giving organisations reason to assess their post-quantum exposure well before the threat becomes urgent. Across these risks, long-term advantage will depend on secure digital foundations, adaptable supply networks and governance that connects strategic investment to mission consequences.

53%

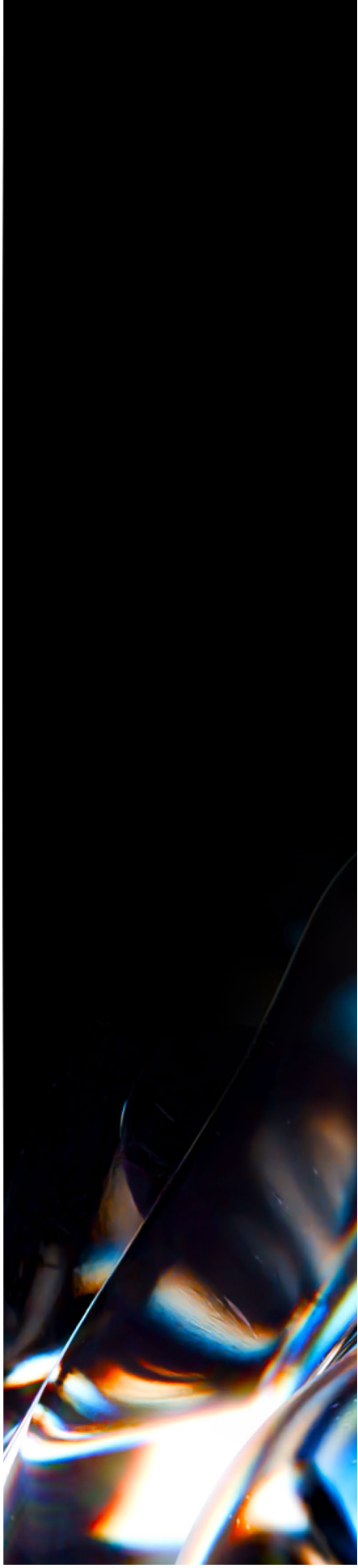
Security and privacy remain the most frequently selected risk theme.

Top long-term risks – A&D leaders



Calls to action for A&D leaders

- **Connect** transformation, protection and response planning across programmes, contracts, technical requirements, supply chains and mission outcomes.
- **Anticipate** shifts in defence priorities, regulation, trade, alliances and conflicts through scenario planning and early-warning indicators.
- **Modernise** legacy platforms, ERP environments and engineering systems to reduce technical debt and enable secure innovation.
- **Protect** classified data, controlled technical information, intellectual property and operations across primes and lower-tier suppliers.
- **Embed** AI in engineering, coding, programme operations and business workflows where it can expand capacity and mission value.
- **Prepare** engineers, programme teams and business staff to use AI with sound judgement and accountability.
- **Govern** AI according to classification, mission sensitivity, model risk and third-party exposure.
- **Map** qualified suppliers and jurisdictional dependencies, with contingencies for export controls, tariffs and geopolitical disruption.
- **Align** portfolios and capital with mission priorities, emerging technologies, replenishment needs and platform relevance.
- **Use** alliances, exports, licensing and local production to expand allied capacity without weakening oversight.
- **Close** technology-skills gaps through succession planning, technical training and AI-enabled workforce strategies.
- **Assess** post-quantum exposure across long-lived systems, sensitive data and infrastructure before modernisation timelines compress.



About the survey

Our 15th annual **Executive Perspectives on Top Risks and Opportunities Survey** contains insights from 1,330 board members and C-suite executives around the world regarding their views on:

- Ability to transform and protect the enterprise and respond to market opportunities and risks;
- Opportunities for growth considering the current environment;
- Priorities perceived as most critical to maximising the value of AI deployments;
- The top risks on the horizon for the near-term (two to three years ahead) related to 30 specific risks across three dimensions (transform, protect and respond);
- A discussion of their organisations' near-term strategic investment priorities, given the opportunities and the risks they face; and
- The long-term horizon based on 11 risk themes that encompass the 30 near-term risk issues.

Our survey participants shared their views through an online survey conducted in June and July 2026.

About the author



David Brand, Ed.D., is Managing Director and Global Aerospace, Defence & Federal Industry Leader for Protiviti. He has extensive experience in technology auditing, compliance, business leadership, analytics and reporting, risk management, financial controls and board reporting. He is one of Protiviti's founding members and has held numerous leadership positions, including leading the Chicago Internal Audit Practice, the Central United States Internal Audit Practice, the Global IT Audit Practice, serving as Atlanta office leader and East Region leader, and now leading Protiviti's Global Aerospace, Defence & Federal Industry practice.

Contact David at david.brand@protiviti.com.

Protiviti (www.protiviti.com) is a global consulting firm that helps clients transform and protect their businesses, and respond to planned and unexpected events. Through a network of more than 90 offices in over 25 countries, Protiviti and its independent and locally owned member firms deliver deep expertise and tailored capabilities across technology, artificial intelligence, data, operations, finance, legal, compliance, HR, marketing, digital, risk, and internal audit—enabling organisations to accelerate innovation, navigate risks and safeguard what matters most.

Named to the Fortune 100 Best Companies to Work For® list since 2015, Protiviti Inc. has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

© 2026 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans.
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. 1026

protiviti®