



The 2026 State of Agentic AI Cyber Risk Report

Jan 2026

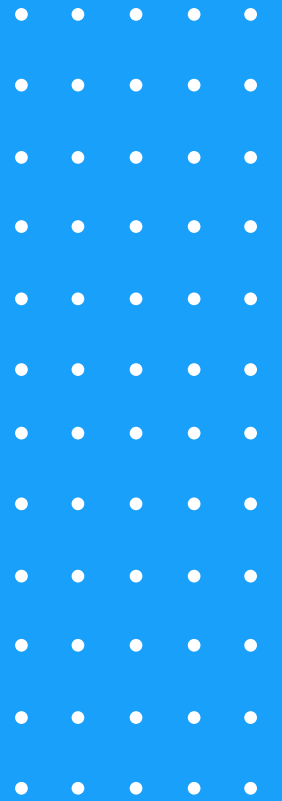


Table of Contents

Introduction and Key Findings 3

Survey Report Findings..... 6

Would damage from an attack targeting agentic workflows be worse than traditional cyber tactics? 7

Prevalence of attacks involving AI agents or autonomous workflows..... 8

Current level of agentic AI adoption within the company 9

Have security or data concerns impacted the deployment of AI agents or autonomous systems in the past year? 10

Is your organization torn between AI adoption and innovation goals and cybersecurity priorities? 11

Strongest internal advocates for deploying agentic AI solutions 12

Who holds primary accountability for managing AI-related cybersecurity risks? 13

Relative difficulty of detecting and containing agentic-workflow attacks vs. traditional attacks..... 14

Cyber threats perceived to cause the greatest existential damage to the organization 15

Key cybersecurity threats the organization is most prepared to manage 16

Confidence in current tools and knowledge to manage agentic AI cyber risks 17

Planned 2026 cybersecurity investment changes to address AI or agentic risks..... 18

Perceived vendor responsiveness to AI cybersecurity risks..... 19

What are the most likely macro-level consequences if agentic cyber risks remain unaddressed?..... 20

Demographics.....21

About Apono 23

Introduction and Key Findings



Introduction & Methodology

Organizations across industries see the potential for AI to fundamentally change how they operate. The promise is clear: faster execution, reduced manual work, and the ability to scale decision-making in ways that were previously impossible.

But the mood has shifted since the first wave of experimentation. Security leaders are increasingly recognizing that while AI can accelerate business outcomes, it can just as easily accelerate risk of attack.

In many organizations, the biggest barrier to broad adoption is not the technology itself. It's the recognition that existing security gaps become more dangerous once AI systems are operating inside the environment. Privileged access, identity governance, and visibility into who or what can access sensitive resources are emerging as the primary sources of concern.

This tension is playing out internally. Technical and security leadership often see the competitive advantage AI can deliver and are pushing to move faster. At the same time, they are confronting the fact that existing controls were designed for a very different world. Tools and processes that struggle to manage human and non-human identities today are unlikely to hold up once autonomous systems begin making access decisions at machine speed.

What is becoming clear is that AI does not introduce entirely new security problems. Instead, AI amplifies the deficiencies that already exist. Weak identity governance, overprivileged access, and limited visibility into permissions become far more consequential once decisions and actions are automated and carried out at scale.

As a result, many organizations are pausing. They still believe in the value of AI, but they don't want to move forward on an unstable foundation.

For security leaders, this is a pivotal moment. It's an opportunity to address long-standing gaps in identity and access management, not as a defensive exercise, but as a way to unlock the full potential of AI safely. With a clear view of current posture and controls designed to scale with change, teams can move from hesitation to confidence.

Those that take action now will be better positioned to adopt AI deliberately and securely. With the right access controls in place, AI becomes what it was always meant to be: a force multiplier that accelerates innovation rather than a source of unchecked risk.

Methodology

To better understand how organizations are approaching agentic AI adoption and the associated cybersecurity risks, Apono commissioned a global survey of 250 senior cybersecurity professionals. The research was conducted by Global Surveyz, an independent market research firm, and completed in December 2025.

Participants were drawn from organizations with 250 or more employees across the United States, Canada, the United Kingdom, Germany, France, Italy, and the Middle East and Africa region. Participants were recruited through a global B2B research panel and invited via email to complete the survey. All responses were collected during December 2025. The average time to complete the survey was 7 minutes and 8 seconds. To reduce potential order bias, the answer order for most non-numerical questions was randomized.

Key findings

01 | Only 2% of cybersecurity leaders have faced agentic AI attacks, yet 100% agree the fallout would be worse than a traditional cyberattack.

Concern about agentic AI risk is already widespread, despite most companies admitting they have not had direct experience with these kinds of attacks. All respondents agree that attacks targeting agentic workflows would be more damaging than traditional cyber threats, despite 98% reporting they have not yet experienced or observed such an incident firsthand. This gap matters. It suggests organizations understand that once systems can act autonomously, mistakes and attacks scale differently, creating a short window to put the right controls in place before incidents become widespread.

02 | Agentic AI is a top-tier threat but not a top-tier capability

Agentic AI attacks rank among the top three threats respondents believe could cause the most serious damage, yet they do not appear even among the top six threats organizations feel prepared to manage, with only 21% reporting readiness. This contrast highlights how quickly agentic AI has moved into the risk conversation ahead of operational maturity. Teams recognize the potential impact, but preparedness, tooling, and clear security models have not yet caught up. Almost all organizations are increasing their investment in this area this year to meet this need, on average by 18%.

03 | Agentic AI is entering production under heightened security scrutiny

Agentic AI is already in use across most organizations, with 57% deploying it in specific workflows and 42% still in testing or prototype phases. At the same time, nearly all respondents report that security and data concerns have slowed deployments, added review steps, or reduced project scope. This indicates that agentic AI is moving into production before security teams feel fully prepared. As a result, we can see caution in play, and 98% of respondents agree that security and data concerns have caused significant slowdowns, added review steps, or other bottlenecks. Organizations need to decide what “safe” looks like when software can reason, decide, and act autonomously.

04 | AI adoption and security accountability are pushing in different directions

Agentic AI adoption is most often driven by CIO and CTO leadership, while accountability for AI-related cyber risk sits primarily with CISOs and security teams. At the same time, 98% of cybersecurity stakeholders agree their organization feels friction between accelerating AI innovation and meeting cybersecurity priorities. This gap matters because the pressure to move fast and the responsibility for managing risk do not sit with the same roles. That misalignment becomes most visible as agentic systems move closer to production, forcing teams to navigate competing priorities without a shared operating model.

Survey Report Findings



Would damage from an attack targeting agentic workflows be worse than traditional cyber tactics?

Cybersecurity stakeholders showed unanimous agreement that attacks targeting agentic workflows would cause greater damage than traditional cyber tactics. The majority (51%) strongly agreed, with the remaining 49% somewhat agreeing, and no neutral or opposing responses.

The lack of disagreement is notable. Security teams are already aligned that attacks involving agentic workflows represent a higher-impact threat than those they manage today, in large part due to the potential scale of these attacks.

This reflects a clear understanding that systems able to act autonomously, moving data, executing tasks, and triggering workflows, create fundamentally different failure scenarios. Even without extensive real-world incidents to draw from, respondents recognize that when these systems are compromised, the potential impact is broader, faster, and harder to contain.

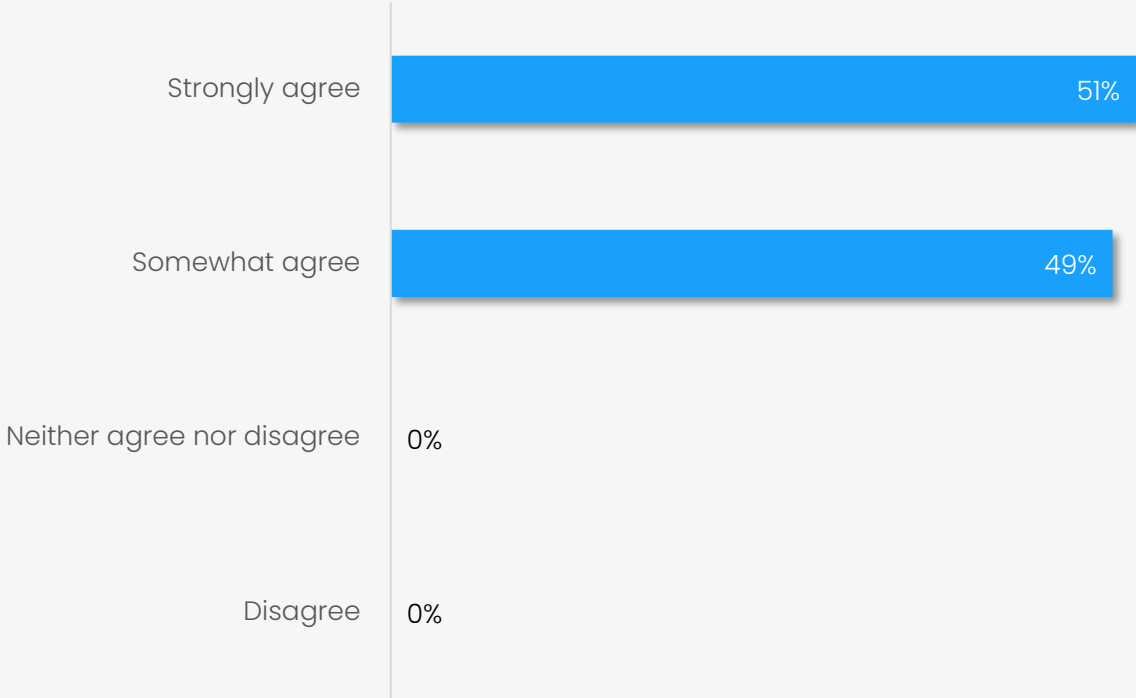


Figure 1: Potential scale of damage from an attack targeting agentic workflows is much higher compared to traditional cyber tactics

Prevalence of attacks involving AI agents or autonomous workflows

Reported cyber incidents involving AI agents or autonomous workflows remain rare among respondents. Nearly all cybersecurity stakeholders (98%) said they have not experienced or observed such an incident, and only 2% reported one occurring within the past six months.

This likely reflects how early most organizations are in deploying agentic AI with meaningful autonomy. These systems have not yet been in widespread, high-impact production long enough for many teams to encounter failures firsthand.

Importantly, low incident rates should not be interpreted as low risk. Instead, they point to a narrow window of opportunity. Organizations still have time to make deliberate decisions about how much autonomy agents should have, where guardrails belong, and what controls must be in place before responsibility is expanded.

The greatest risk at this stage is complacency, assuming that limited exposure means limited action is required. In reality, this is the period when preparation can have the greatest impact and leverage for an organization.

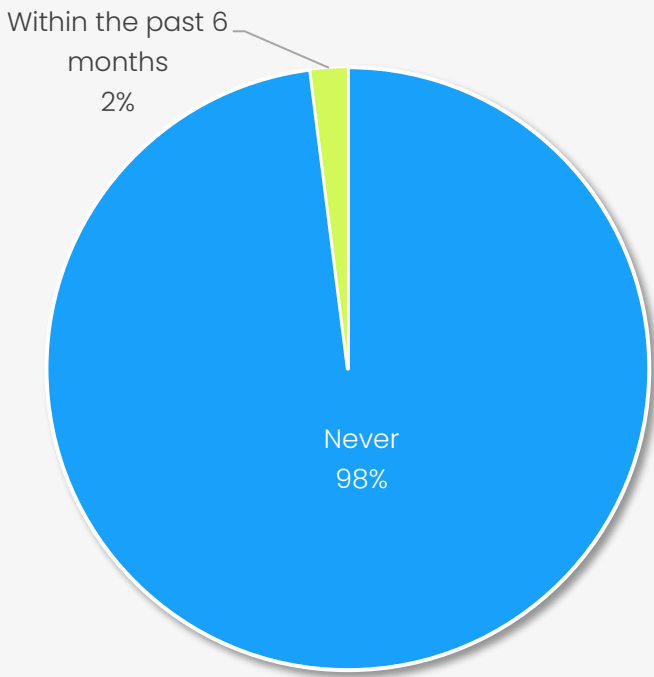


Figure 2: Recency of cyber incidents experienced or observed involving AI agents or autonomous workflows

Current level of agentic AI adoption within the company

Agentic AI adoption remains early-stage for most organizations. A majority of respondents (57%) report limited use within specific workflows, while 42% say they are still in testing or prototype phases. Only a negligible share report expanded use across teams (0.5%) or organization-wide deployment (0.5%), indicating that broad-scale adoption is still rare.

The data shows that agentic AI is already present inside organizations, but deployment is cautious. Most teams are experimenting or confining agents to narrowly defined use cases rather than scaling broadly.

At the same time, the near absence of expanded or organization-wide use suggests that organizations are still working to understand the implications before increasing autonomy or reach.

Importantly, even limited deployment changes the security equation. Once agents are active in production workflows, containment becomes a temporary condition, not a guarantee, and the need for clear security controls becomes immediate.

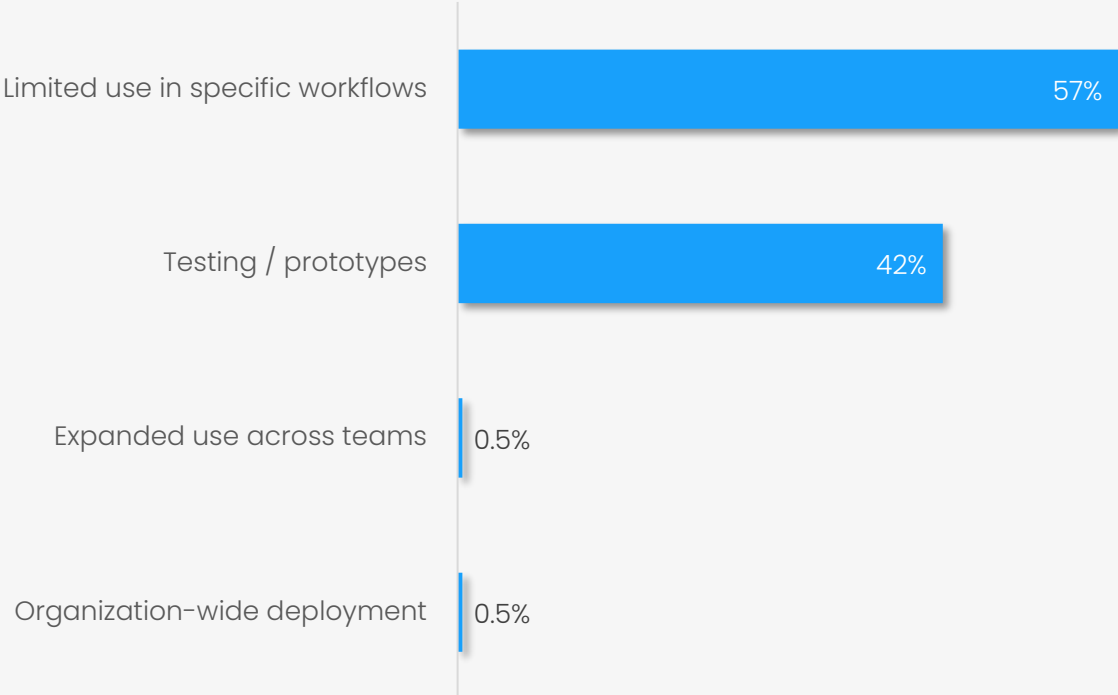


Figure 3: Current level of agentic AI adoption within the company

Have security or data concerns impacted the deployment of AI agents or autonomous systems in the past year?

Most cybersecurity stakeholders (77%) reported slowdowns or additional review steps in the deployment of AI agents and autonomous systems this year, while 21% said these concerns led to significant delays or reduced project scope. Only 2% experienced minor adjustments with no impact on timelines, and virtually none reported no impact or no related discussion.

The takeaway is straightforward: security concerns are shaping how agentic AI projects move forward for almost every organization. Whether through added reviews, slower rollouts, or narrower initial scope, risk considerations are influencing deployment decisions.

Interestingly, this may not reflect resistance to agentic AI itself. In most cases, development continues, just with greater caution and more checkpoints. Organizations are not saying “no,” but rather “not yet,” “not everywhere,” or “not without stronger safeguards.”

This dynamic helps explain why adoption remains uneven. Uncertainty around how to deploy agents safely, without introducing new classes of risk, is acting as a natural constraint on scale.

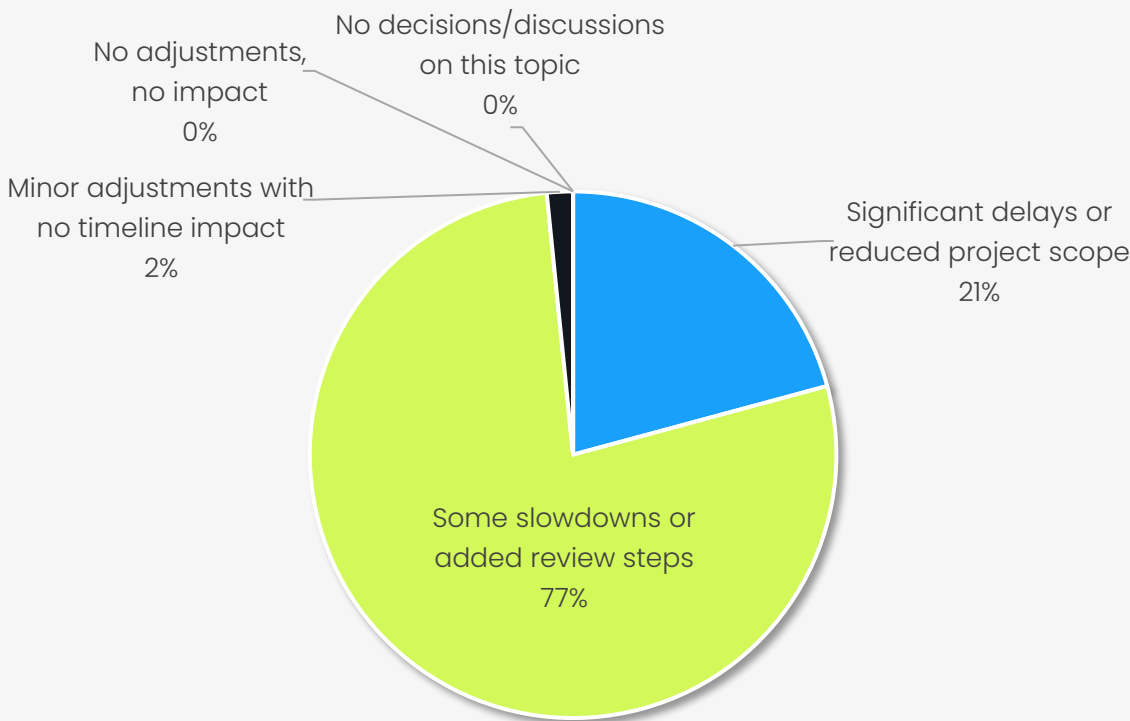


Figure 4: Impact of cybersecurity or data-security concerns on deployment of AI agents or autonomous systems in the past year

Is your organization torn between AI adoption and innovation goals and cybersecurity priorities?

Respondents overwhelmingly perceive tension between accelerating AI adoption and meeting cybersecurity priorities. Nearly all participants (98%) agree that this friction exists, with 33% strongly agreeing and 65% somewhat agreeing. Only 1% were neutral and 1% disagreed.

This reflects a shared experience across roles and levels: organizations feel pulled in two directions. There is strong pressure to move AI agents toward production and take advantage of the next big thing, alongside equally strong pressure to slow down and manage risk.

The result is a careful, deliberate pace. Innovation continues, but the push and pull shows up in the way that decisions are made with increased scrutiny as teams try to balance speed with security.

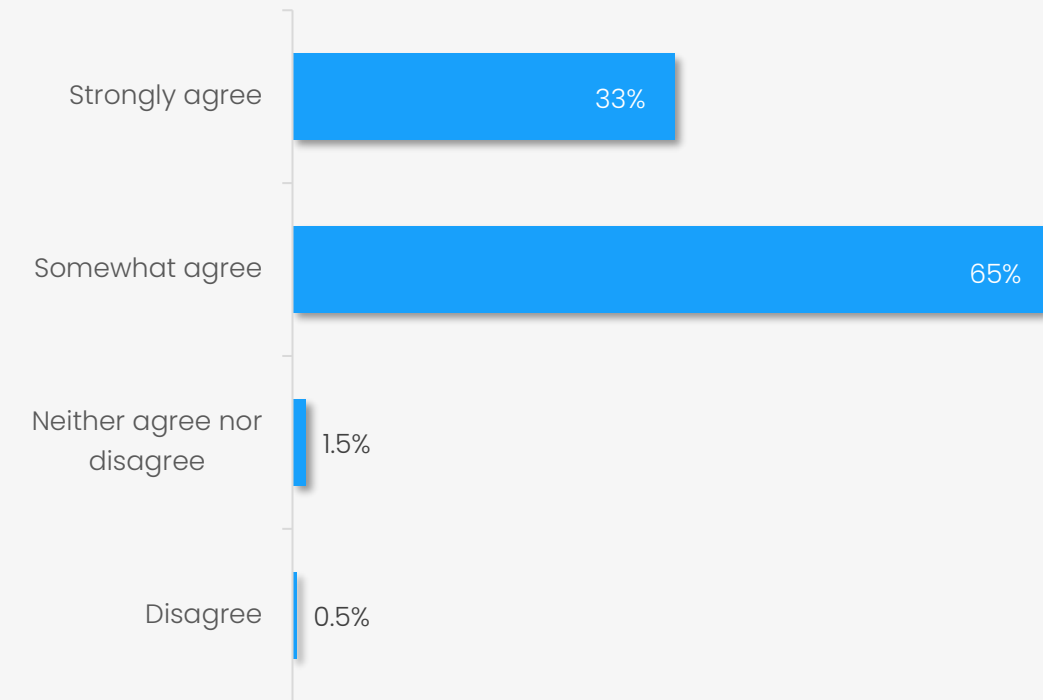


Figure 5: Agreement that the organization is torn between AI adoption/innovation goals and cybersecurity priorities

Strongest internal advocates for deploying agentic AI solutions

Advocacy for deploying agentic AI is heavily concentrated within technical leadership. CIO and CTO roles are most frequently cited as the strongest internal advocates (45%), followed by CISO and security leadership (34%) and CEO or board-level leaders (21%). Notably, the strongest advocates are leaders closest to infrastructure and risk. This points to a deliberate push toward agentic AI led by those who understand both its potential and its security implications.

No respondents identified line-of-business leadership, external consultants, or the absence of a clear advocate. **This finding may partly reflect the perspective of the respondents themselves.** As all participants were cybersecurity professionals, they may naturally view technical leadership as the primary drivers.

Nevertheless, the concentration suggests that momentum is being driven from the top of the technical organization rather than from bottom-up demand or vendor pressure. The absence of line-of-business advocacy indicates that agentic AI is not yet being pulled into the organization by operational teams.

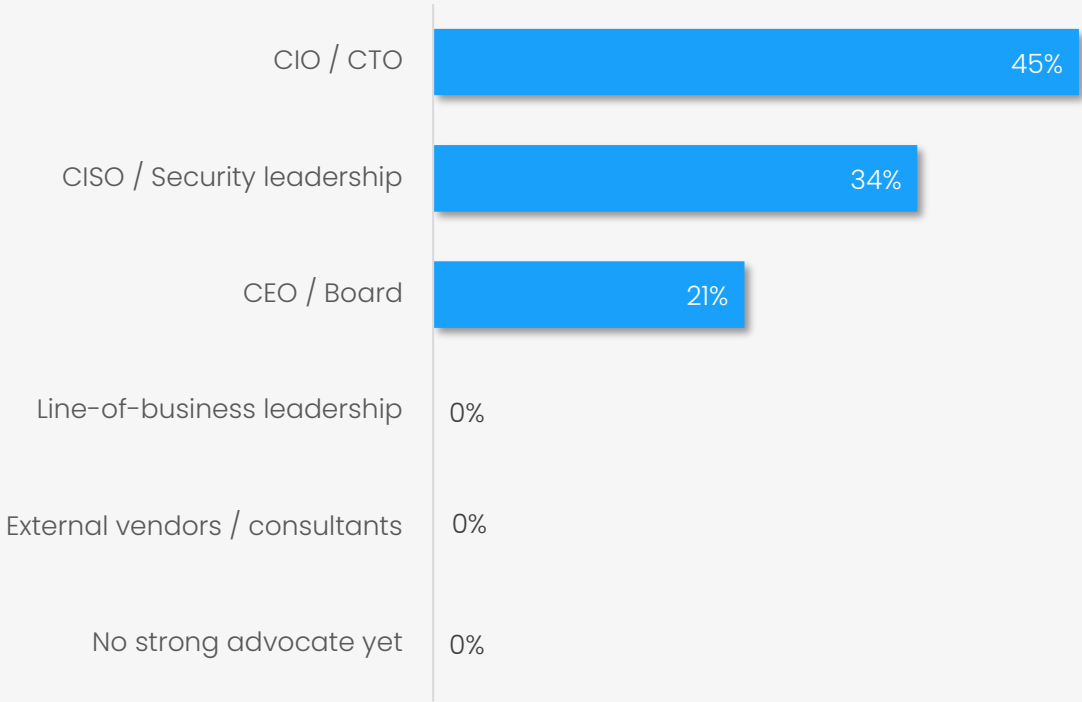


Figure 6: Strongest internal advocate for deploying agentic AI solutions within the organization

Who holds primary accountability for managing AI-related cybersecurity risks?

Primary accountability for managing AI-related cybersecurity risk sits squarely with the security function. A large majority of respondents (77%) identify CISO or security leadership as the primary owner, while CIO or CTO roles are cited as secondary owners by 23%. No other functions were selected.

This indicates a clear consensus that AI-related cyber risk is a security responsibility first and foremost. While technology leadership plays a supporting role, accountability is not distributed broadly across the organization, underscoring the central role security teams are expected to play as agentic AI adoption advances.

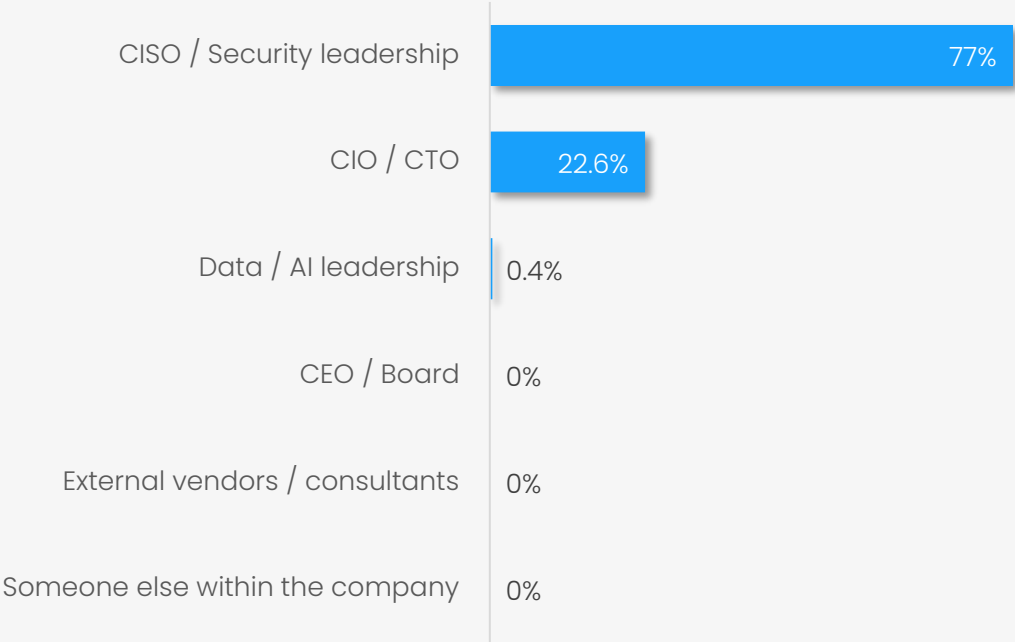


Figure 7: Primary accountability for managing AI-related cybersecurity risks within the organization

Relative difficulty of detecting and containing agentic-workflow attacks vs. traditional attacks

Cybersecurity stakeholders overwhelmingly expect attacks involving agentic workflows to be harder to detect and contain than traditional cyber threats. Nearly all participants (99%) anticipate greater difficulty, with 73% saying detection and containment would be slightly harder and 26% saying much harder. Only a negligible share expect no change (0.6%) or an improvement (0.4%).

This reflects a clear expectation that existing detection and response approaches will not translate cleanly to agent-driven systems. Security teams are already anticipating more complex investigations and slower containment when autonomous agents are involved.

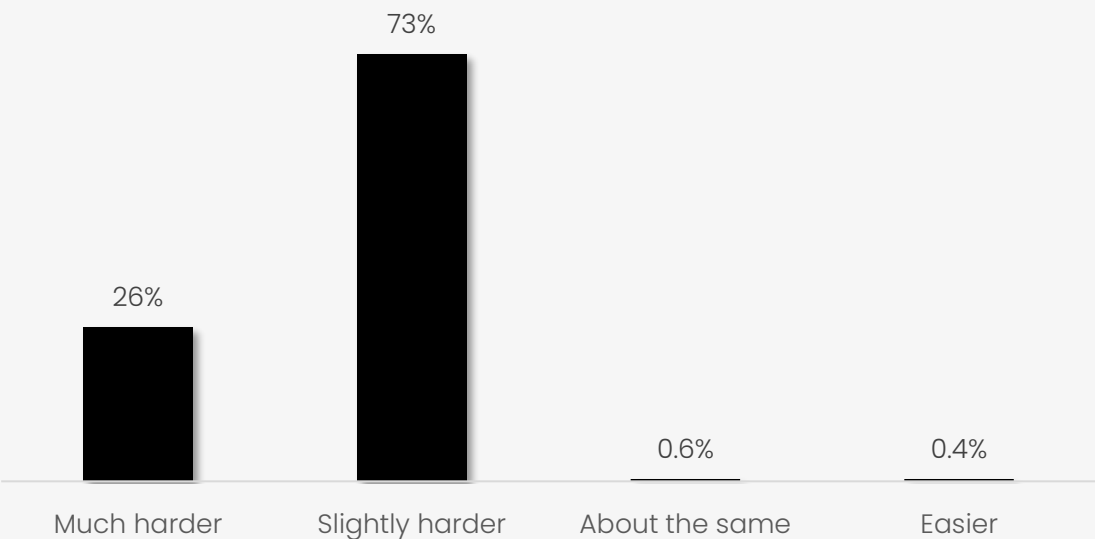


Figure 8: Relative difficulty of detecting and containing agentic-workflow attacks vs. traditional attacks

Cyber threats perceived to cause the greatest existential damage to the organization

Respondents most often identify ransomware or malware (72%) and third-party or supply chain breaches (68%) as the cyber threats most likely to cause existential damage. This is unsurprising as they are familiar threats with well-understood consequences. However, attacks involving agentic AI or autonomous workflows rank next (48%), placing agentic threats among the top-tier threats organizations are considering.

This indicates that agentic AI is not being viewed as a niche or theoretical concern. While more established threat categories still rank highest, agentic attacks are already being grouped with the types of incidents leaders believe could cause serious organizational harm, even though almost no organizations have faced them yet.

Concern varies by seniority. Managers (68%), heads of function (57%), and directors (52%) are significantly more likely to rank agentic AI attacks as existential risks than VP-level leaders (22%) or individual contributors and team leads (15%), suggesting prioritization increases with responsibility.

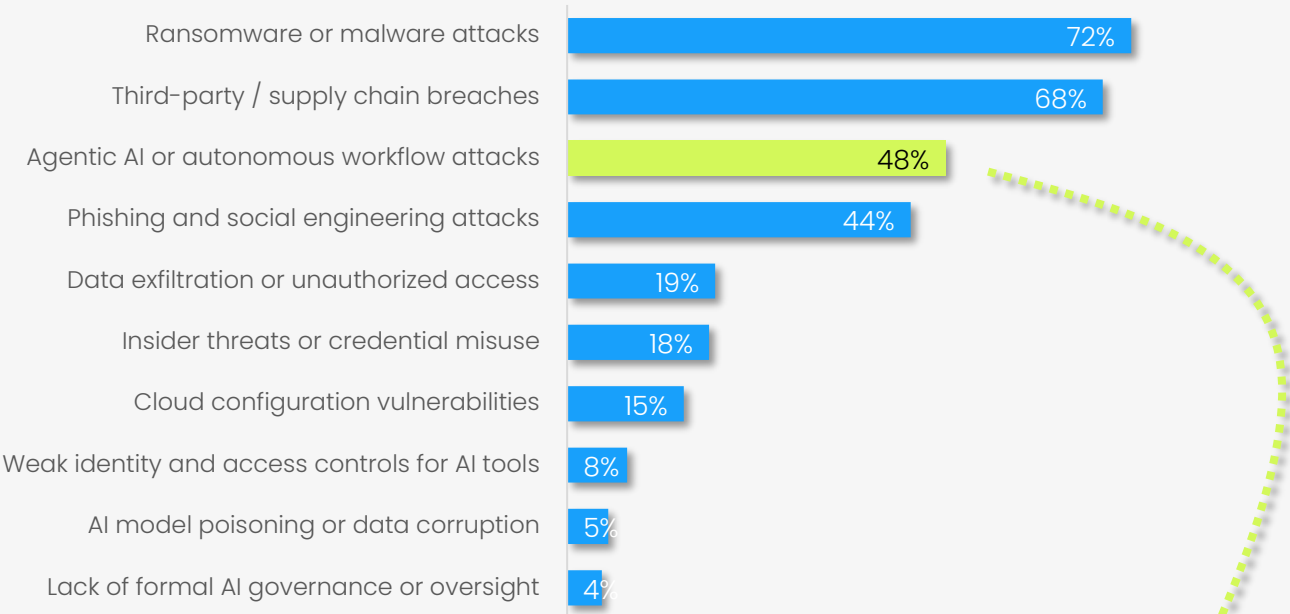


Figure 9: Cyber threats perceived to cause the greatest existential damage to the organization

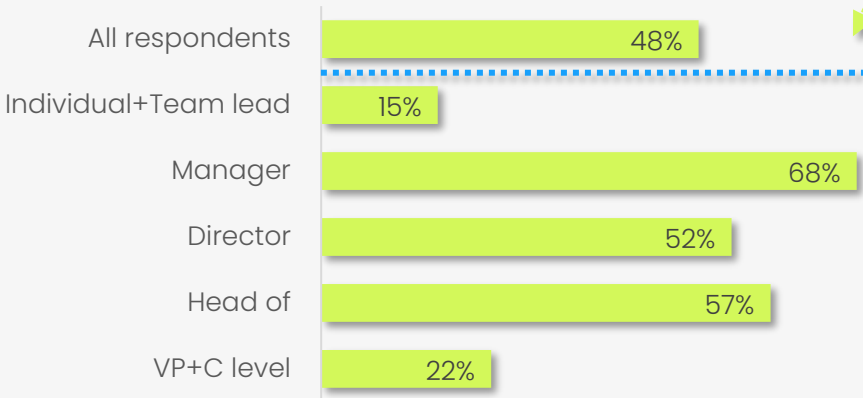


Figure 10: Agentic AI or autonomous workflow attacks by job seniority

*Question allowed more than one answer and as a result, percentages will add up to more than 100%
The 2026 State of Agentic AI Cyber Risk Report 15

Key cybersecurity threats the organization is most prepared to manage

Organizations report the highest level of preparedness for traditional, well-understood threats. Respondents most often cite readiness for cloud configuration vulnerabilities (62%), phishing or social engineering (55%), and ransomware or malware (54%), followed by insider threats or credential misuse (42%).

In contrast, only 21% say they are prepared to manage attacks involving agentic AI or autonomous workflows, highlighting a significant preparedness gap. Agentic threats do not even rank among the top six areas where teams feel operationally confident.

Preparedness perceptions also vary by seniority. Individual contributors and team leads (30%) and VP-level leaders (30%) report the highest confidence, while managers (17%), directors (22%), and heads of function (16%) are less likely to say their organization is ready. This pattern suggests confidence decreases as accountability for outcomes increases. Those closer to owning outcomes seem less convinced the organization is ready.

While traditional threats may feel manageable because teams have seen them before, agentic AI does not yet fall into that category.

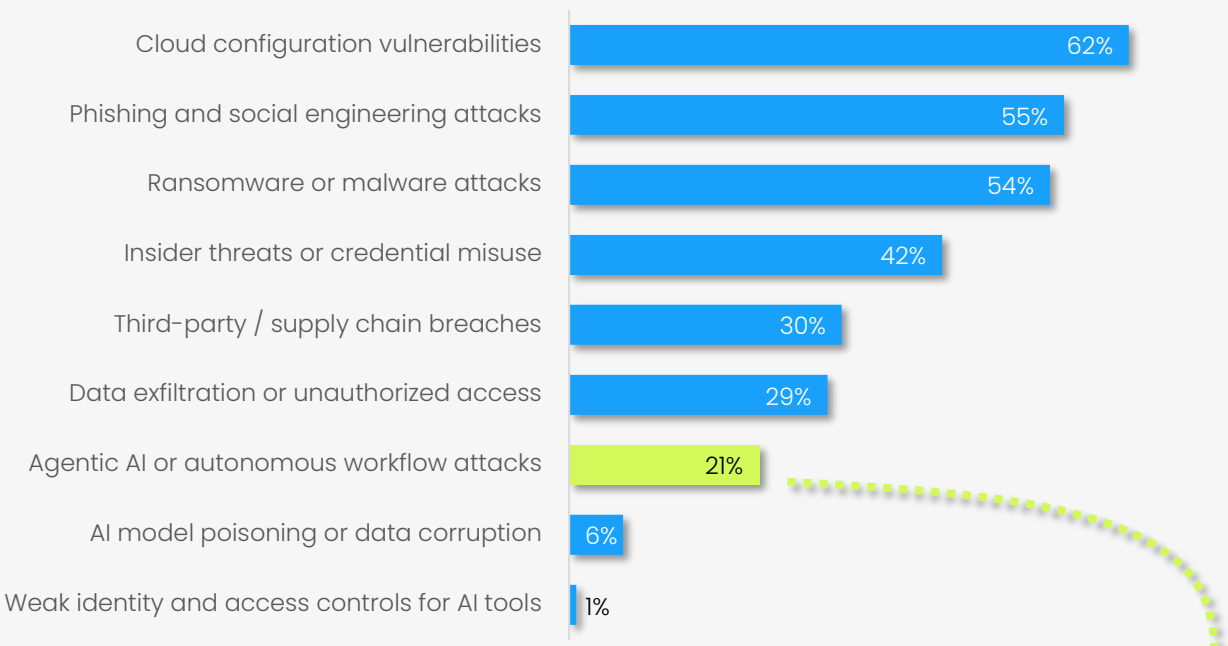


Figure 11: Key cybersecurity threats the organization is most prepared to manage effectively

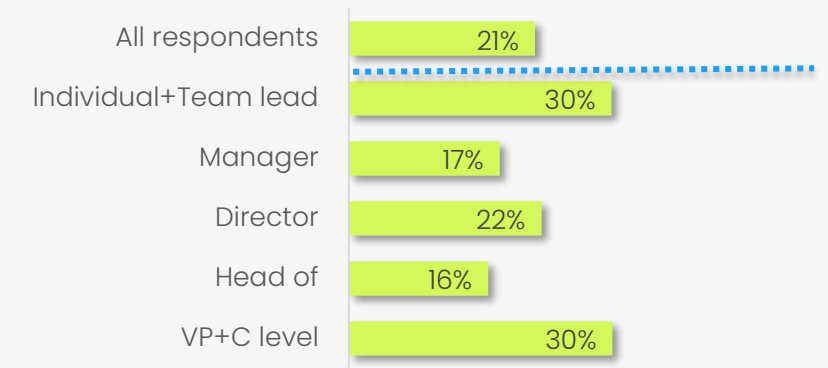


Figure 12: Agentic AI or autonomous workflow attacks by job seniority
*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Confidence in current tools and knowledge to manage agentic AI cyber risks

Confidence in current tools and knowledge to manage cyber risks from agentic AI systems is mixed and generally modest. Half of respondents (50%) report being somewhat confident, while nearly as many (46%) say they are not very confident. Only 1.5% feel very confident, highlighting the immaturity of the security function in facing this new and growing threat.

The distribution suggests most organizations may believe they have some baseline capability, but not enough to feel secure. As very few respondents express strong confidence, this helps explain why deployments move cautiously and why additional reviews and slower timelines are common when agentic systems approach production.

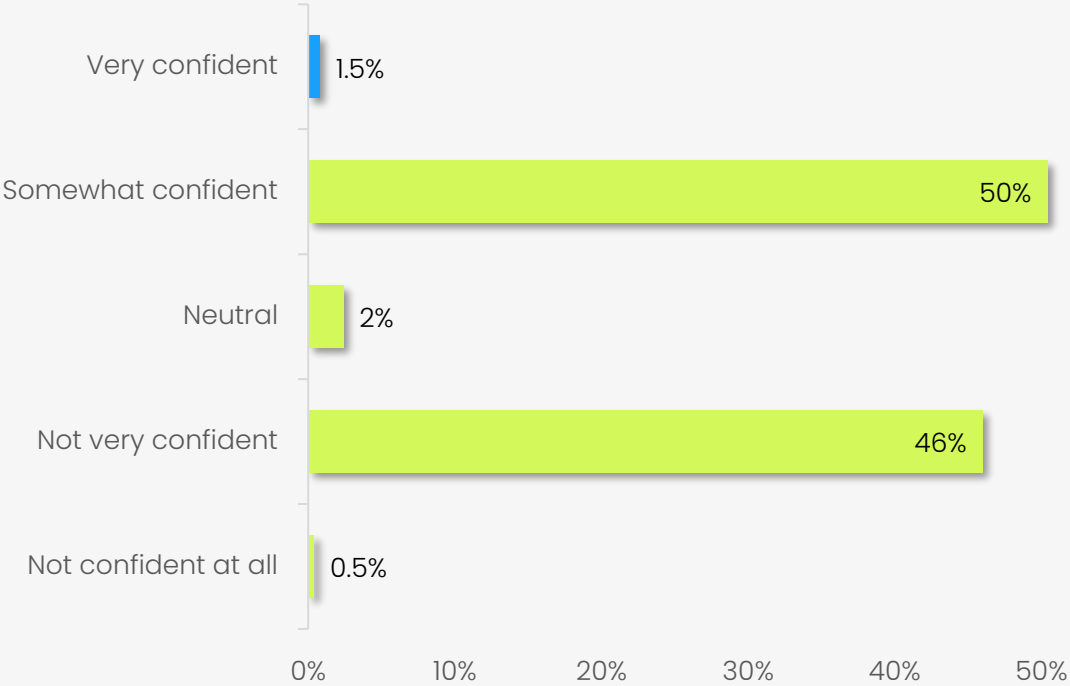


Figure 13: Confidence in the organization’s current tools and knowledge to manage cyber risks of agentic AI systems

Planned 2026 cybersecurity investment changes to address AI or agentic risks

Organizations are planning to increase cybersecurity investment in 2026 to address AI- and agentic-related risks. A majority (60%) expect a slight increase of 1–25%, while the remaining 40% anticipate a significant increase of 26% or more. No respondents plan to keep spending flat or reduce investment, with the average planned increase at 18%.

This indicates broad budget momentum toward strengthening defenses against emerging AI-driven threats. While most organizations are opting for incremental increases rather than major jumps, the absence of flat or reduced spending suggests agentic risk is being treated as a sustained priority rather than a temporary concern.

Teams are willing to spend, even if they’re still finalizing exactly where that money should go to have the greatest impact.

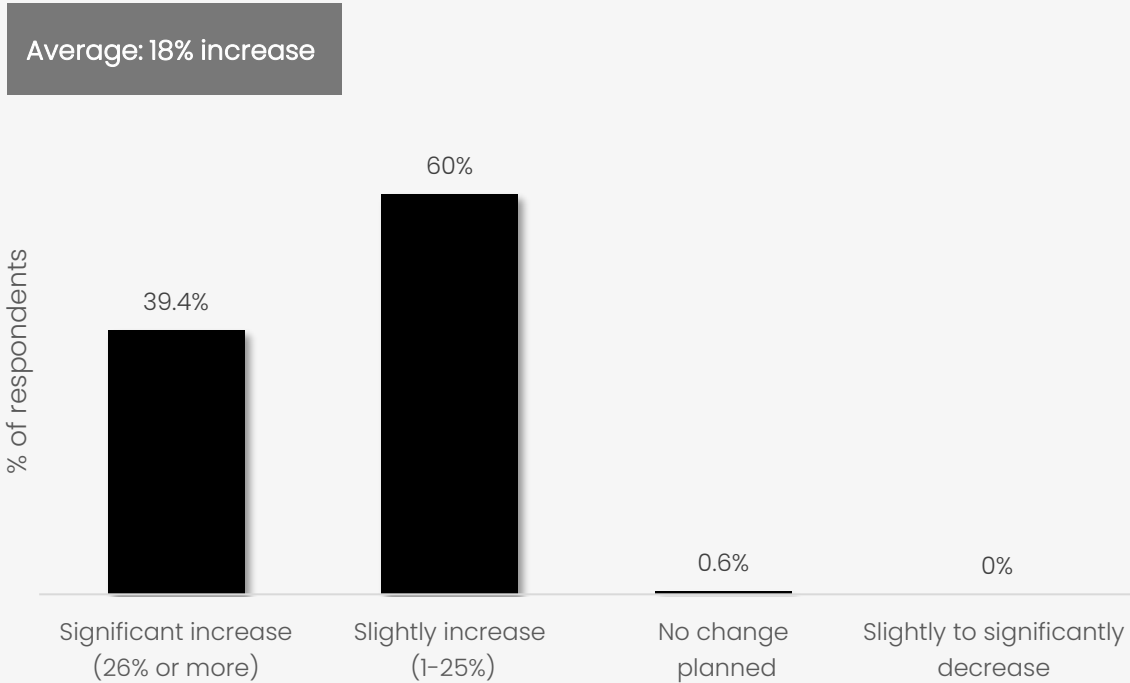


Figure 14: Planned 2026 Cybersecurity Investment Changes to Address AI- or Agentic-Related Risks

Perceived vendor responsiveness to AI cybersecurity risks

Respondents consistently perceive a gap between vendor awareness and action on AI cybersecurity risks. All participants (100%) describe vendors such as Anthropic, Google, OpenAI, and Microsoft as aware of these risks but overly optimistic, with no respondents viewing vendors as transparent and proactive, or as downplaying or discouraging discussion.

This indicates that while vendors acknowledge the existence of AI-related cyber risk, customers do not yet see a corresponding level of urgency or concrete action. The perception sits squarely between denial and leadership.

This reinforces a broader pattern in the data: organizations do not yet feel there is a mature, trusted ecosystem to support the secure adoption of agentic AI, even as pressure to deploy these systems continues to increase.

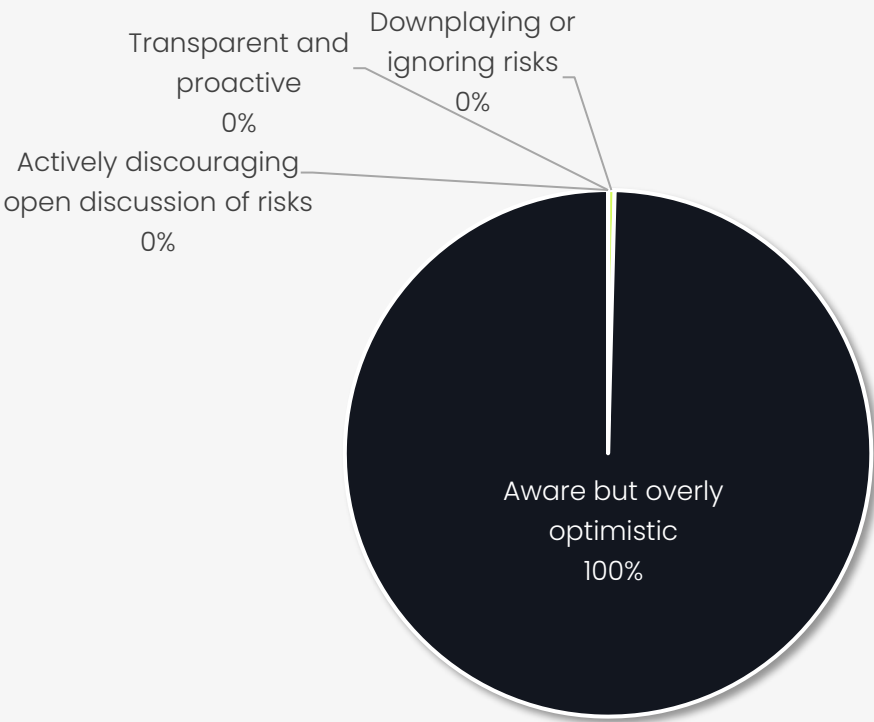


Figure 15: Perceived Vendor Responsiveness to AI Cybersecurity Risks

What are the most likely macro-level consequences if agentic cyber risks remain unaddressed?

Respondents expect the most severe macro-level consequences of unaddressed agentic cyber risk to be systemic in nature. The top concern is a breakdown of critical infrastructure (74%), followed by acceleration of AI-driven cyber threats (62%) and declining public trust in agentic systems (50%).

Secondary concerns include increased regulatory intervention or market fragmentation (46%) and geopolitical instability or escalation of cyber warfare (34%).

Overall, the data shows concern is focused less on localized disruption and more on cascading, system-level consequences. Security failures in agentic AI are seen as having the potential to undermine trust, accelerate threat activity, and disrupt critical systems at scale.

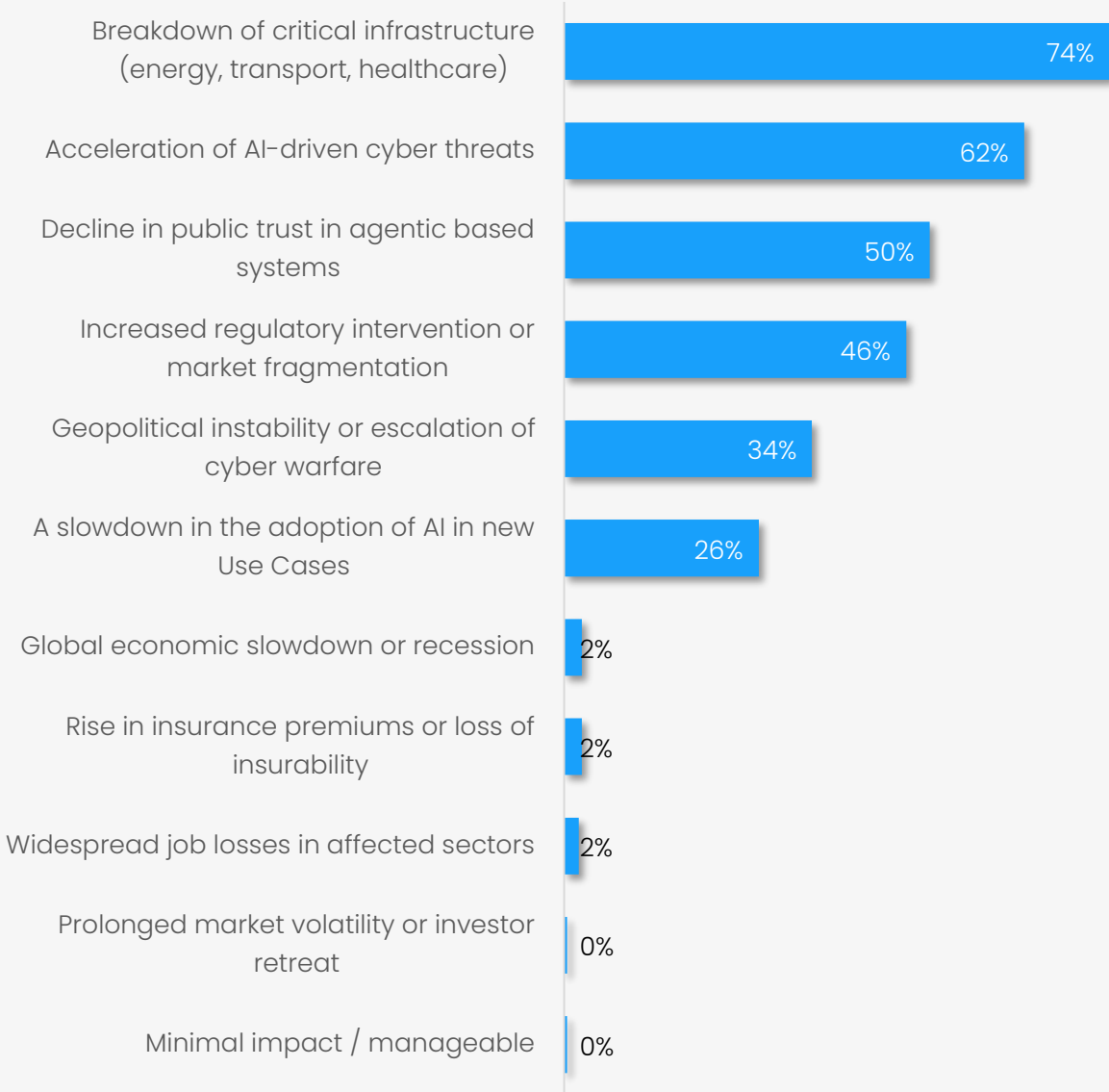


Figure 16: Most likely macro-level consequences if agentic cyber risks remain unaddressed

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Demographics



Country, Industry, Company size, Department, Job seniority

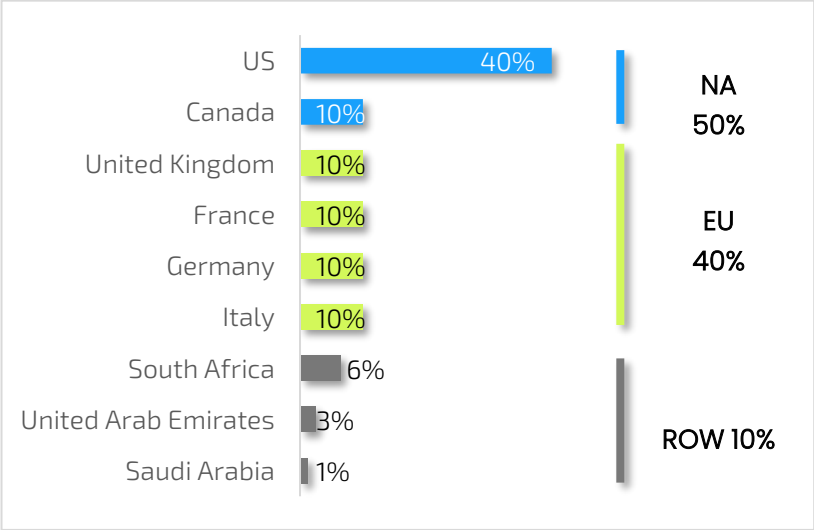


Figure 17: Country

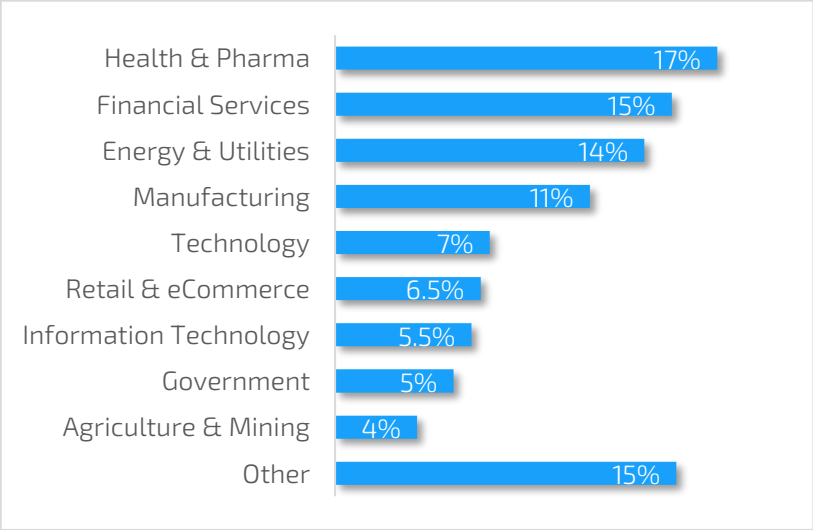


Figure 18: Industry

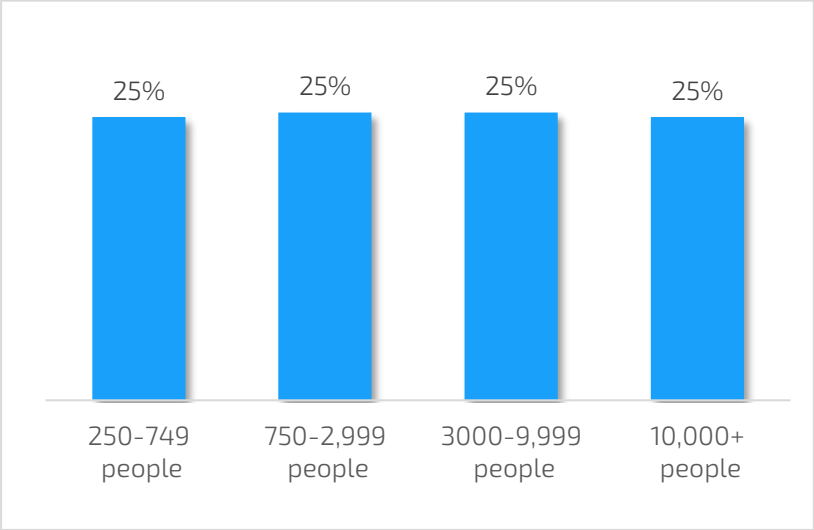


Figure 19: Company size

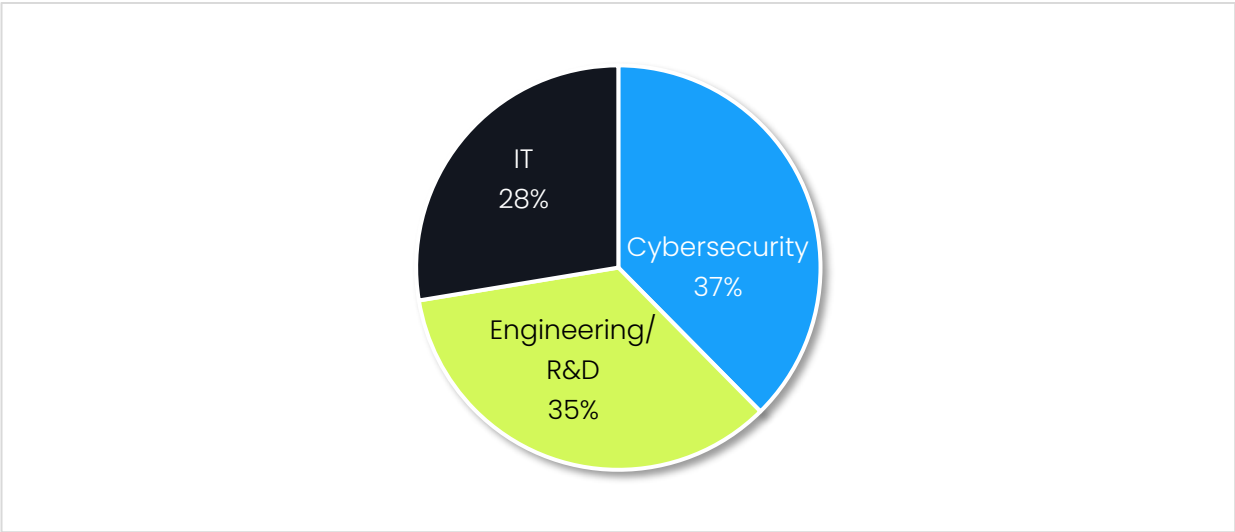


Figure 20: Department

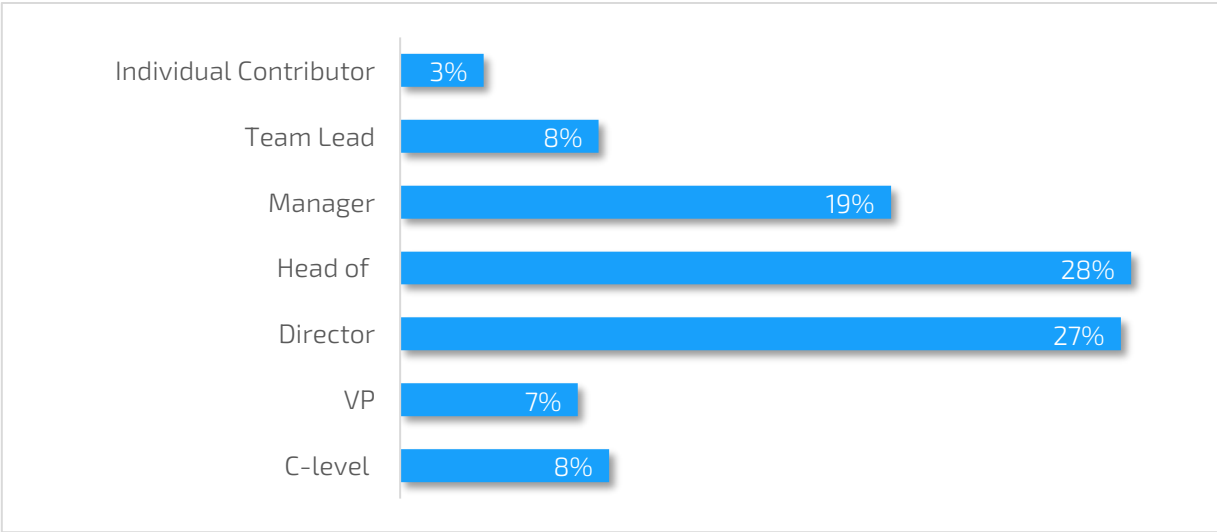


Figure 21: Job seniority

About Apono

Apono is a cloud identity-security company helping enterprises manage and control access across complex, modern environments. Founded in 2021 by cybersecurity and DevOps experts, the company provides automated permission-management solutions that enforce Zero Standing Privileges with Just-in-Time and Just-Enough Access models access models. Apono's

platform is designed to give security and infrastructure teams fine-grained visibility and control over cloud permissions while maintaining compliance and minimizing operational friction. The company is headquartered in New York, with an additional office in Tel Aviv, Israel.

[Request a Demo](#)

Visit us at:



www.apono.io

Phone: +1 (626)548-6178 | Email: info@apono.io