servicenow

2026 Risk and security outlook

How AI is reshaping enterprise risk and security

© 2026 ServiceNow, Inc. All Rights Reserved.

Preface

Ben de Bont

Chief Information Security Officer
ServiceNow

Risk has always been a part of doing business, but its scale, speed, and impact are changing. What once could be managed within discrete functions is now embedded across platforms, workflows, and decisions, shaped by accelerating technology change, growing interconnection, and persistent uncertainty. The 2026 Risk and Security Outlook examines how this shift is changing the risk environment.

Based on a global survey of 1,000 risk and security leaders across industries, we found that technology and AI now sit at the center of the global risk landscape. Digital transformation, cloud migration, and the rapid spread of generative and agentic AI are widening attack surfaces and introducing new vulnerabilities, often faster than defenses can adapt.

At the same time, with tightly connected digital ecosystems and global markets, failures rarely stay contained. A cyber incident, system outage, or regulatory shock in one area can cascade quickly, amplifying impact and compressing response time.

While many executives expect some external pressures, such as macroeconomic volatility and regulatory change, to stabilize in the year ahead, the center of gravity is shifting inward. Organizational weaknesses, including skills gaps, fragmented governance, misaligned teams, and immature risk systems, are increasingly determining whether threats are absorbed or escalate into disruption.

Readiness is not keeping up with exposure. Even as adversaries rapidly weaponize AI, many organizations report limited confidence in their ability to manage AI-enabled threats. Our report unpacks these dynamics to show where risk is intensifying, how preparedness varies by industry and region, and what leaders are doing to close the resilience gap.

© 2026 ServiceNow, Inc. All Rights Reserved.

A changing risk landscape

servicenow

Technology is reshaping the risk landscape

Over the last three years, technology and AI risks have risen sharply, making today's global risk landscape more unpredictable, interconnected, and complex.

Technology and data sharing have woven organizations into dense digital ecosystems where internal systems, vendors, platforms, and partners are tightly linked. A cyber incident or service failure in one area can cascade rapidly through supply chains, financial flows, and customer channels, turning a local problem into a system-wide disruption. The interconnectivity of global markets compounds the problem.

This interconnectivity of digital systems and world markets, combined with technology's speed, drives greater unpredictability in the risk environment. Chain reactions erupt across digital networks and global markets through dependencies and feedback loops, causing risks to emerge unexpectedly and suddenly.

The AI effect

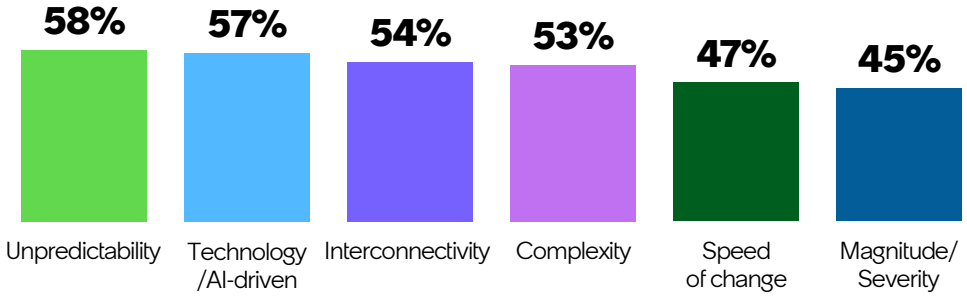
While AI can help control these risks, if used incorrectly, it can do the opposite by inserting opaque systems into critical decisions, operations, and infrastructures. AI models are often trained on imperfect data, which makes errors, bias, and model drift difficult to detect before they cause harm. Worse, AI can amplify cybersecurity and fraud threats by giving adversaries the ability to launch more effective phishing, ransomware, and disinformation campaigns, which can damage reputations and profits.

Industries in the eye of the storm

While technology risks affect all industries, some sectors are more exposed because of their heavy reliance on digital infrastructure and access to sensitive data. Telecommunications, technology, and financial services are three such industries.

Increase in risk across dimensions

% reporting higher risk in these areas than three years ago



© 2026 ServiceNow, Inc. All Rights Reserved.

Tech risks will continue to rise over the next 12 months

On balance, executives expect technology and cyber risks to stay frothy over the next 12 months. Today's dynamic interplay of risks from inside and outside organizations creates a more challenging environment for executives. Technological and organizational weaknesses make it harder to handle shocks from the outside, while external risks expose and worsen internal weaknesses.

Growing risks within the organization

Over the next 12 months, the biggest risks will come from within organizations. For almost six in 10 executives, the shift to integrated digital platforms will magnify dangers from system failures, cyber vulnerabilities, and misconfigurations. Most executives expect risks from shadow AI and insider threats to grow as the use of digital and AI technology spreads.

Unfortunately, organizational weaknesses could intensify technological risks over the next 12 months. Just over half of organizations expect skill shortages to grow, undermining digital competence and cybersecurity. And without alignment between security and business teams, many executives worry that risk management will be less effective.

A more stable external risk environment

Overall, executives expect calmer external conditions. Most believe that financial and business risks will stay the same or lessen. And they also feel similarly about climate and energy disruptions and government intervention. But there are some rising consumer, economic, and geopolitical uncertainties on the horizon that could cloud the picture.

Risk by category	% rising	% same or falling
Technology and cyber risk		
Technology systems and platforms	59%	41%
Shadow AI and IT	52%	48%
Insider threats	52%	48%
AI adoption (offensive and defensive uses)	49%	51%
Cyberattacks and data breaches	48%	52%
Disinformation/Loss of trust	46%	54%
Leadership and talent risks		
Talent and skills shortages	51%	49%
Alignment of security and business teams	49%	51%
Leadership, governance, and internal controls	41%	59%
Market and economic risks		
Changing customer needs/demographics	53%	47%
Macroeconomic volatility	51%	49%
Supply chain and third-party ecosystem	49%	51%
Financial stability and performance	47%	53%
Business growth and scale of operations	44%	56%
Speed of innovation/new competitors	44%	56%
Geopolitical and regulatory risk		
Geopolitical instability/terrorism	50%	50%
Climate and energy disruptions	46%	54%
Regulatory change/government intervention	45%	55%

© 2026 ServiceNow, Inc. All Rights Reserved.

Risk expectations vary by industry

Higher risks

Technology, financial services, consumer goods, and telecoms anticipate higher risks across each risk domain over the next 12 months—with the highest being technology risks as accelerated digital innovation expands their attack surfaces. Consumer goods firms also anticipate rising technology risks, as well as considerably higher risks from changing consumer needs and economic volatility.

Stable to higher risks

Healthcare, government, and retail organizations all expect higher technology risks over the next 12 months. Healthcare and retail also see greater risks from changing customer needs and supply chain disruptions. Government agencies expect greater threats from climate change and geopolitical instability.

Stable risks

Automotive, nonprofit, insurance, and life sciences organizations foresee a relatively stable risk environment for 2026. Even in areas flagged as higher risk for these industries, the risk intensity is more subdued than it is for other industries.

Risk level	Ranked by industry	Technology and cybersecurity	Organization and talent	Market and economic	Geopolitical and regulatory
Higher	1. Financial	Higher	Higher	Higher	Higher
	2. Technology	Higher	Higher	Higher	Higher
	3. Consumer	Higher	Higher	Higher	Higher
	4. Telecoms	Higher	Higher	Higher	Higher
Stable to higher	5. Healthcare	Higher	Stable	Higher	Stable
	6. Government	Higher	Stable	Stable	Higher
	7. Retail	Higher	Stable	Higher	Stable
Stable	8. Automotive	Stable	Stable	Higher	Higher
	9. Nonprofit	Higher	Stable	Higher	Stable
	10. Insurance	Higher	Stable	Stable	Stable
	11. Life sciences	Stable	Stable	Higher	Stable

© 2026 ServiceNow, Inc. All Rights Reserved.

The biggest risks organizations face and how they will address them

Technology and cyber risks

"

Shadow AI will be our biggest challenge, so **we are using centralized AI governance and approval."**

CFO
Indian insurance firm

Organizational risks

"

Talent retention is a growing challenge. Keeping that in mind, we are offering flexible work options and career development programs to keep employees engaged."

Senior executive
KSA telecoms firm

Market and economic risks

"

Biggest risk is margin pressure from rising input costs and supply chain volatility. **We are mitigating this through automation investments, cost optimization initiatives, and strategic hedging."**

Senior executive
Canadian consumer goods company

Geopolitical and regulatory risks

"

The major risk we face is geopolitical instability. To control this, **we are expanding partnerships and scenario planning."**

Senior executive
Indian government agency

© 2026 ServiceNow, Inc. All Rights Reserved.

AI is raising the stakes

servicenow

Cyber adversaries are weaponizing AI

Executives expect AI innovation to amplify cyber risks for organizations over the next 12 months as adversaries capitalize on AI's growing capabilities. The largest jumps in threat intensity will come from three cyber areas:

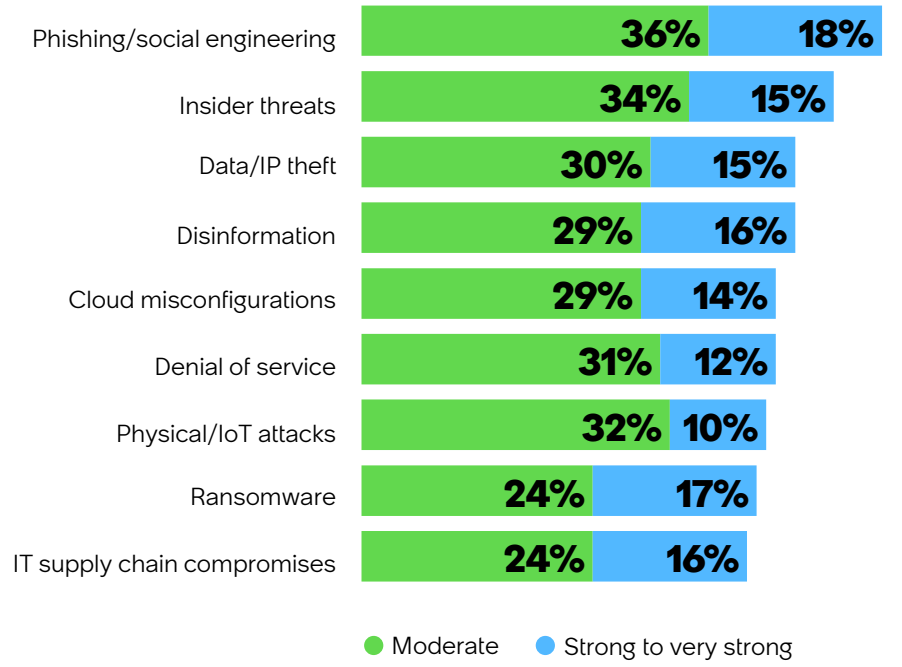
- **Phishing attacks,** as adversaries use AI to generate highly personalized and grammatically correct emails and deepfake messages at scale
- **Insider threats due** to employee use of AI tools and platforms with greater access to corporate data
- **Data/IP theft,** as adversaries leverage AI to scale attacks, bypass controls, and extract sensitive data and IP more rapidly

Other areas of greater attack

Many executives also worry about rising threats from disinformation, cloud misconfigurations, and denial of service as attackers automate and scale what used to require skilled humans.

Using AI tools, adversaries can quickly locate and extract valuable data and intellectual property from sprawling cloud and SaaS environments, especially those that are poorly configured. At the same time, generative and agentic AI make it more difficult for organizations to distinguish real information from carefully crafted manipulation.

% expecting moderate to very strong increase in threat intensity from the use of AI by cyber adversaries



© 2026 ServiceNow, Inc. All Rights Reserved.

AI threats are rising faster than organizational defenses

AI may be accelerating the capabilities of attackers faster than the defense mechanisms of organizations. Indeed, most executives in our study report only very low to moderate confidence in handling AI-enabled threats across all attack vectors.

Executives are least confident in mitigating AI-enabled intrusions through the following attack vectors:

- **Cloud misconfigurations,** which AI can more easily identify and exploit than before
- **Insider threats,** boosted by AI's ability to analyze and capitalize on inappropriate staff behaviors
- **Ransomware attacks,** which can be automated and masked through AI
- **Disinformation,** made more convincing with AI
- **Data and IP theft,** which adversaries can supercharge by using AI to find weaknesses in digital systems and platforms

Confidence varies by industry. Government organizations tend to have low confidence because of the ability of AI-enabled adversaries to outmaneuver their fragmented legacy IT systems, inadequate AI governance mechanisms, and understaffed IT teams. With their focus on speed and innovation over security, many technology firms feel they may be losing the AI arms race with cybercriminals.

Very low to moderate confidence in mitigating AI threats by attack vector

AI threats by attack vector	% of executives	Industry lows
Cloud misconfigurations	57%	Government, tech: 65%
Insider threats	55%	Government: 63%
Ransomware	55%	Government: 64%
Disinformation	55%	Government: 64%
Data/IP theft	55%	Technology: 62%
Physical/IoT attacks	53%	Technology: 61%
IT supply chain compromises	52%	Government: 65%
Denial of service	51%	Automotive: 58%
Phishing/Social engineering	50%	Technology: 65%

"We might face misconfiguration of cloud services, so it will be **necessary for us to perform regular risk assessments."**

Senior executive, German life sciences firm

© 2026 ServiceNow, Inc. All Rights Reserved.

GenAI and agentic AI pose new risks to the uninitiated

More than 80% of organizations now use generative AI (GenAI) and agentic AI. While these new forms of AI can drive significant value for organizations, they can also usher in new dangers, even when used for risk management.

Managing risks from GenAI and agentic AI

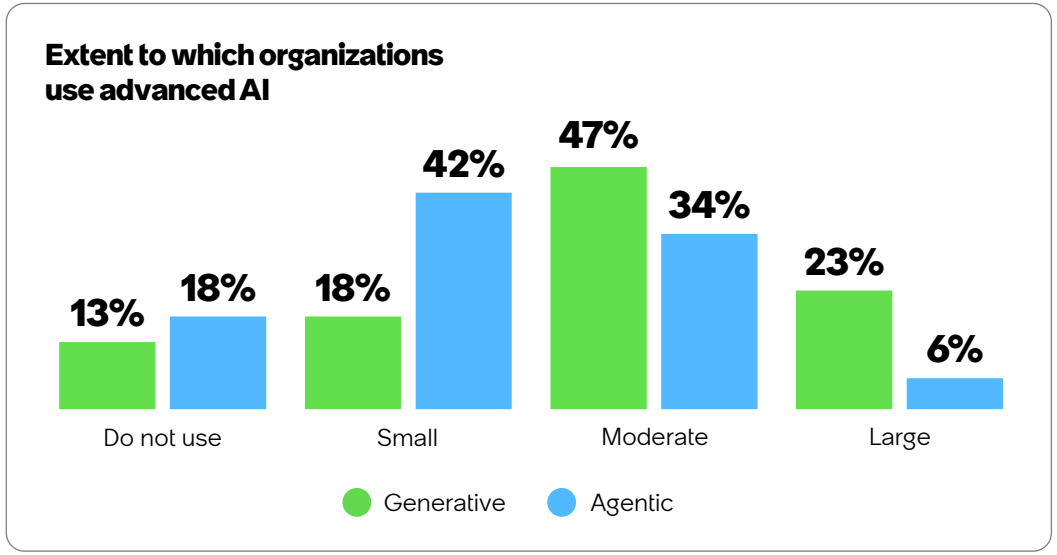
Unfortunately, many organizations are not yet confident in their ability to mitigate the risks resulting from the adoption these new technologies. Almost half of executives report very low to moderate confidence in avoiding biased or unfair outputs from the latest AI models. Almost as many are unsure that they have the full capabilities to mitigate the risks from loss of human oversight, malicious use AI, or model drift.

Some sectors are ill-prepared

In a likely case of "what you don't know won't hurt you," organizations that have been slower to adopt GenAI and agentic AI, such as those in the nonprofit, healthcare, and life sciences sectors, tend to be more confident about their ability to fend off the associated AI risks. Conversely, industries that have made the greatest use of GenAI and agentic AI—and have the most knowledge—such as technology, telecoms, and consumers goods, tend to be less confident.

"The biggest risk we face over the next 12 months is associated with the increasing use of generative and agentic AI."

Senior executive, US tech firm



© 2026 ServiceNow, Inc. All Rights Reserved.

Many organizations are not AI ready

servicenow

Many are no more prepared for risk than they were 12 months ago

Despite the rise in technology, market, organizational, and regulatory risks, only 52% of the organizations in our survey took steps to prepare more for risk over the last 12 months. The remaining organizations—for which progress has halted or even deteriorated—face a dangerous, widening gap between the level of risk they face and the risk management capabilities they possess.

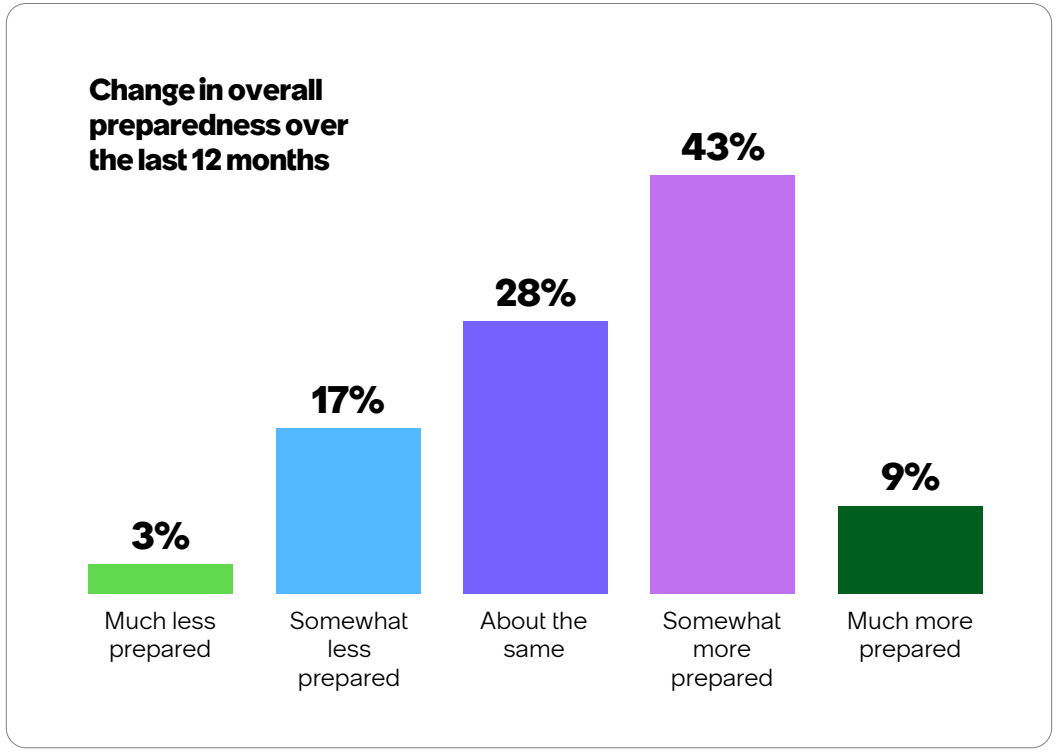
Industries that prepared the most

Over the last year, life science firms have been exposed to rising national security and cyber regulations, growing geopolitical and trade pressures, and escalating cyberattacks on high-value IP and clinical data. To cope with this fast-changing risk and the regulatory landscape, life sciences firms have increased their risk and security preparedness more than organizations in any other industry over the past 12 months.

Similarly, under pressure from regulators to protect financial assets, financial services and insurance firms have stepped up risk preparedness over the last 12 months. Retailers, which have faced well-publicized and extremely damaging cyberattacks in the past year have also made notable progress in improving their preparedness.

Industries that prepared the least

Other industries have done less to prepare for the risks ahead. A case in point is consumer goods companies. Many have rushed into e-commerce and direct-to-consumer models, often without updating IT architecture and risk governance, leaving blind spots for disruptions and cyber threats. In addition, with less board involvement in risk issues than other industries, consumer goods firms have less risk-readiness pressure from the top.



© 2026 ServiceNow, Inc. All Rights Reserved.

Confidence in security posture is lacking

With many risk management systems failing to keep pace with a fast-changing, tech-driven risk environment, it is hardly surprising that executives are losing confidence in their future ability to protect their businesses from the dangers ahead.

Preparedness = confidence

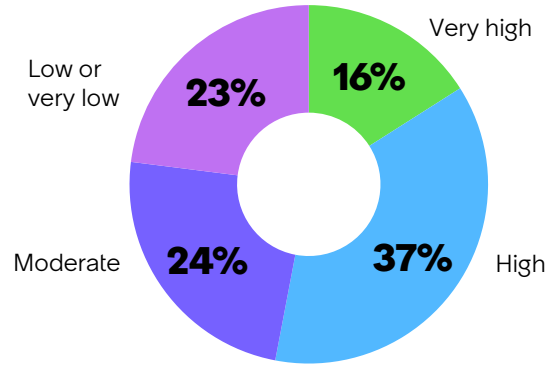
Almost half of the organizations in our study—typically from industries that did less to prepare—report low to moderate confidence in their risk posture over the next 12 months. This leaves them in a vulnerable position if risks grow in 2026, as some executives believe they may.

Industry and regional trends

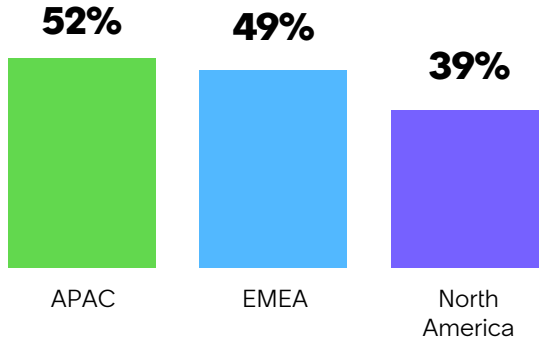
Telecoms, consumer goods, and automotive companies have the lowest confidence in their risk resilience, largely because they have done the least to prepare for risks over the last 12 months. In contrast, life sciences, financial services, and insurance companies have done the most to prepare, hence they have greater confidence.

Overall, APAC organizations are the least confident, whereas North American organizations are the most. This is due in part to the smaller size of organizations and budgets in APAC. But it also reflects greater regulatory pressures, talent shortages, and looser controls.

Almost half of organizations have very low to moderate confidence in their security and risk posture



% of organizations by region with very low to moderate confidence



© 2026 ServiceNow, Inc. All Rights Reserved.

Many boards are not on top of emerging risks

Boards have a fiduciary role to safeguard their organizations from harm. But in today's fast-changing, technology-driven risk environment, only 55% of boards have a clear view of risk, according to our research. The percentage is even lower—44%—for smaller organizations with under $5 billion in revenue.

Too often, boards receive fragmented, back-looking analyses that obscure emerging threats and their interdependencies. On top of that, many boards, particularly those in smaller organizations, lack the expertise, risk tools, and governance structures to provide the full guidance needed.

Differences between industries

When boards lack risk awareness or engagement, organizations are more likely to underinvest in critical controls, misjudge strategic trade-offs, and respond too slowly to emerging threats. Our research shows that risk preparedness and board involvement are intrinsically linked.

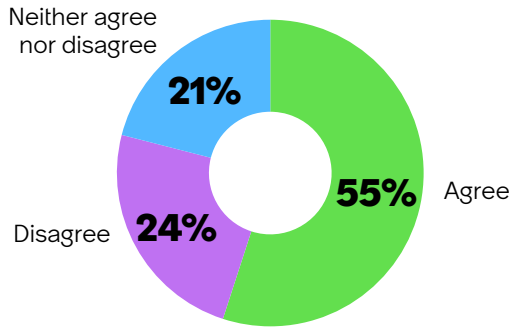
This pattern is reflected in the variations across industries. The six industries where boards are perceived to be more aware of risks are also the six industries that have made the greatest improvements in risk preparedness over the past 12 months.

Industry and regional trends

There is also significant regional variation in boards' understanding of risk and security threats, with North American companies significantly better positioned than their peers in EMEA and APAC. The larger size of U.S. firms, along with stricter corporate governance rules in the U.S., is a factor.

"Our board of directors has a clear and accurate view of the risk and security threats facing our organization."

Respondent agreement with above statement:



© 2026 ServiceNow, Inc. All Rights Reserved.

Key purchasing decisions are concentrated in too few hands

Risk and security technologies—from multifactor authentication to scenario analysis models—are critical elements of an organization's risk defenses. In today's battle to gain an advantage against cyber adversaries, the role of technology in risk management will continue to take on greater prominence.

But as risk becomes more technology driven and multifaceted, decisions regarding which technology solutions to purchase are becoming more complicated. Such decisions require a team approach, which takes multiple perspectives into account.

A heavy burden on too few shoulders

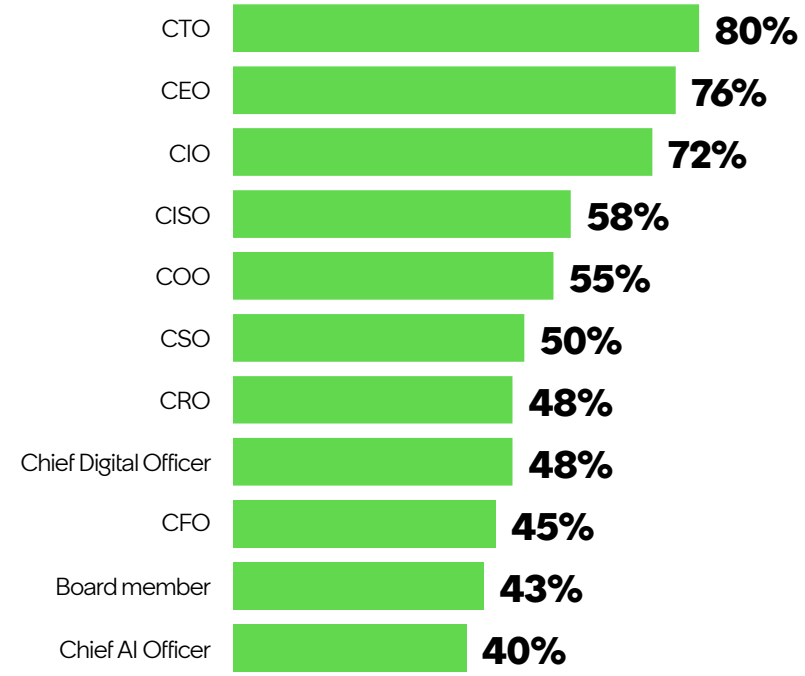
However, our survey shows that risk technology buying decisions are often concentrated in only a few hands. Across industries, top management, including CTOs, CEOs, and CIOs, most often makes buying decisions. This often excludes insights from risk and security executives, such as CISOs, CSOs, and CROs, and AI experts, such chief AI officers.

Where decision-making is more distributed

As with other aspects of risk management, there is substantial variation across industries. In sectors with more mature approaches to risk management, such as banking, telecommunications, and technology, decision-making authority regarding these purchases is far more distributed among executives than it is in other industries.

Comparing decision-making authority

% of organizations whose leaders have high or very high influence over risk technology buying decisions



© 2026 ServiceNow, Inc. All Rights Reserved.

Improving risk readiness

servicenow

How we assessed risk readiness

To understand which sector is the most risk-ready for the changing risk landscape, we analyzed industries across the following areas:

- The rise in risk and security preparedness over the last 12 months
- The level of confidence in their risk and security posture for the next 12 months
- The planned increase in the level of security-related spending over the next 12 months
- How well the board understands risk and security threats
- The level of shared decision-making on risk technology investments among top management and risk, security, and technology executives

Using data from the survey, we scored each industry over each area and then calculated an overall score by averaging the pillars.

© 2026 ServiceNow, Inc. All Rights Reserved.

Industry comparison

Leaders

- **Financial services** is the clear leader in risk readiness, thanks to a jump in preparedness and spending over the last year, combined with strong board involvement and shared influence in risk technology buying decisions.
- **Retail** is also a top risk performer, thanks to a risk-aware board and growing confidence.

Middle of the pack

- **Life sciences and insurance** sit in the middle: Their risk preparedness has improved, but spending over the next 12 months is not keeping up with other industries.
- **Nonprofits** lead in confidence over the next 12 months. Yet they are upping risk spending the least and failing to involve enough executives in risk tech buying decisions.
- **Government bodies** have middling confidence. They did not prepare enough over the last year but plan to outspend other industries over the next 12 months.

Trailing industries

- **Technology and automotive** trail other industries. They suffer from less risk preparedness and confidence, as well as weaker risk oversight by boards. But they both plan to boost spending on technologies to improve their risk resilience.
- **Telecoms, healthcare, and consumer goods** are at the back of the pack, with low overall readiness and limited recent progress, indicating largely reactive approaches to risk rather than integrated risk management programs.

Risk readiness by sector

Industry	Overall ranking	More prepared over the last year	Confidence over the next year	Spending increase over next years	Board view of risk	Level of shared influence
Financial services	**1**	1	3	3	1	1
Retail	**2**	5	3	5	1	7
Life sciences	**3**	3	2	8	3	6
Insurance	**4**	4	5	7	5	4
Nonprofit	**5**	2	1	11	4	11
Government	**5**	7	6	1	5	10
Technology	**7**	6	10	2	8	3
Automotive	**8**	10	8	4	7	5
Telecoms	**9**	8	11	9	9	2
Healthcare	**10**	9	7	10	9	9
Consumer goods	**11**	11	9	6	11	8

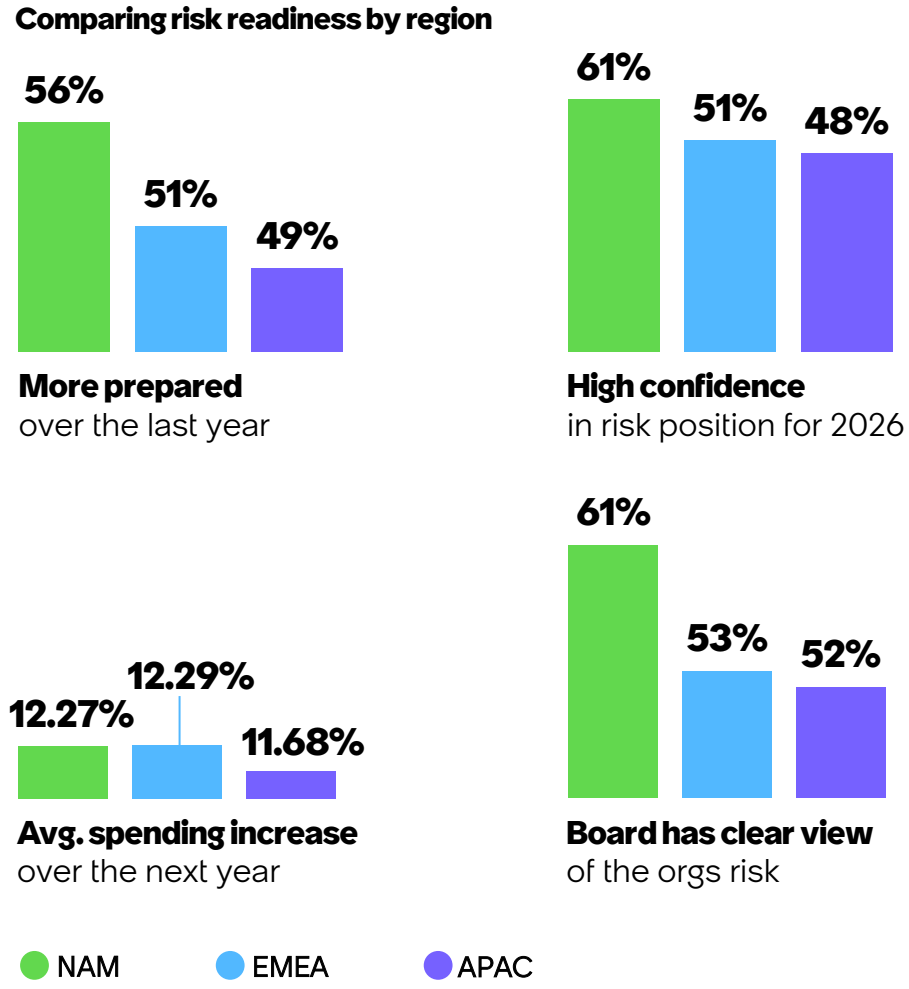
© 2026 ServiceNow, Inc. All Rights Reserved.

Regional comparison

North American organizations show the strongest overall risk posture. Fifty-six percent report feeling more prepared over the last year, and 61% express high or very high confidence in their risk position for the coming year, the highest level across all regions. Because of legal and ownership pressures, boards in North America are more risk aware than those in other regions. .

In **EMEA**, just over half of organizations feel more prepared and a similar share are highly confident about the year ahead. Recognizing the gaps in risk resilience, EMEA organizations plan to make the largest average increase in risk-technology spending at 12.29%, slightly over North America organizations. Board visibility is weaker than in North America, with only 53% reporting a clear view of risks.

APAC organizations have done slightly less than others to prepare for risks over the last year, resulting in less confidence than others over the next year. APAC also expects the lowest average rise in risk-technology spending at 11.68%, which may contribute to more cautious sentiment. Board understanding of risks is relatively limited, with 52% saying their boards have a clear view, underscoring the need for stronger governance to support future resilience.



© 2026 ServiceNow, Inc. All Rights Reserved.

Risk investments: highs and lows

High-investment

Cloud security will see the biggest investment uplift, as organizations shift core workloads and sensitive data to the cloud and face mounting misconfigurations and attacks—and boards take notice.

Executives are also boosting investments in **operational risk tools** to better manage process, people, and systems risks amid supply-chain shocks, cyber incidents, and expanding regulations.

Risk and scenario analysis will also see heavy investment as organizations model interconnected threats—from cyber and fraud to climate and geopolitics—and gauge financial and operational impact.

Low-investment

Most organizations are raising investments in supplier risk management by under 10%. While this may be suitable for industries with less third-party risk, such as nonprofits and healthcare, it could pose problems for companies with complex supply chains.

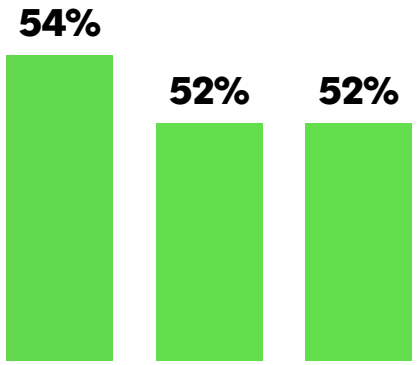
Identity and access management (IAM) will see similarly modest growth, even though identity is one of the main attack vectors today. Assuming IAM work is "finished" can be a serious mistake as bad actors use AI to ramp up identity attacks.

Similarly, not investing enough in **AI-driven threat detection** may give adversaries the advantage in the AI arms race. Nevertheless, organizations are making the lowest investment in this critical area next year.

Comparing technologies: Highest vs. lowest expected investments

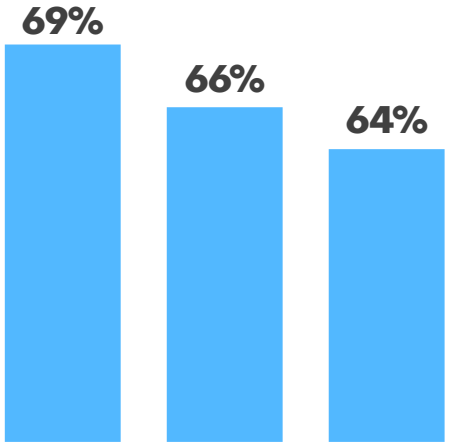
Risk technologies that will see the most investment

% that will increase investment by 10% to over 30% more



Risk technologies that will see the least investment

% of that will increase investment by 0% to up to 9.9%



© 2026 ServiceNow, Inc. All Rights Reserved.

To mitigate risks, executives are investing more in risk tools

To combat burgeoning threats, organizations plan to spend more on risk technology over the next budget cycle, especially in these areas:

- **Cloud and multi-cloud security,** as organizations cope with greater risks from shifting workflows to the cloud
- **Operational risk tools and analysis,** to meet board demands for better real-time risk visibility and management
- **Risk and scenario analysis,** as organizations seek to anticipate cascading shocks and stress-test resilience under increasingly volatile conditions
- **Regulatory-tracking solutions,** to cope with growing rules around data privacy, cybersecurity, AI, and environmental, social, and governance (ESG)

Spending gaps

While these spending increases will no doubt help, they mask a disturbing fact: Many organizations are barely increasing investments in risk technologies; some, not at all.

For example, over half of organizations are making no or only limited investments in regulatory tracking, integrated risk platforms, or business continuity. The percentages are even higher for tools to manage fast-growing risk areas, such as identity management, AI-driven threat detection, and supplier risk management.

Worse yet, a widening divide is emerging between higher spenders—such as technology, government, and financial services organizations—and cash-strapped sectors—such as nonprofit organizations and healthcare providers.

% investment increases in risk management technologies over the next budget cycle

Technology	Avg. rise	% no/low
Cloud security	13.6%	46%
Operational risk	13.1%	48%
Risk and scenario analysis	12.9%	48%
Regulatory tracking	12.8%	51%
Integrated risk platforms	12.6%	51%
Business continuity	12.5%	56%
SOAR	12.2%	55%
Data security tools	11.6%	60%
Training platforms	11.2%	62%
Identity/Access management	11.0%	66%
Supplier risk management	11.0%	69%
AI-driven threat detection	10.7%	64%

© 2026 ServiceNow, Inc. All Rights Reserved.

Five main ways AI can help mitigate risks

AI is a double-edged sword. While it is providing cyber adversaries with new avenues of attack, it is also giving executives better tools to fend off cyber assaults and other risks.

Our analysis of survey responses uncovered five main ways that executives plan to use AI to reduce risks and improve resilience over the next 12 months.

1 Strengthen cybersecurity and data protection

Organizations plan to deploy AI for real-time threat detection, anomaly monitoring, and automated incident response to stop cyber intrusions and mitigate ransomware, phishing, and insider misuse before damage occurs. Organizations will use AI to secure cloud and IoT environments, auto-remediating vulnerabilities to prevent data breaches and outages.

2 Ramp up fraud and financial risk controls

AI models will help executives monitor transactions in real time to flag suspicious behavior, detect money laundering, and identify fraud, reducing losses and protecting trust. Executives will also leverage AI-enabled credit and portfolio risk models to assess default probabilities more accurately, predict liquidity needs, and hedge against price and currency fluctuations, thereby improving financial resilience.

3 Improve operational reliability and supply chain resilience

Organizations intend to use predictive maintenance and condition monitoring to anticipate equipment and network failures, schedule proactive repairs, and avoid unplanned downtime. AI-based demand and supply forecasting will help optimize inventory, route shipments, and monitor vendors, reducing the risk of shortages, logistics delays, and quality defects.

4 Tighten compliance, governance, and reputation management

AI will enable teams to scan policies, contracts, communications, and regulatory updates; monitor global rules,; and run data-integrity checks, lowering legal and regulatory risk. Sentiment and misinformation analysis using AI will help organizations identify emerging reputational threats across social and news channels early and respond quickly.

5 Enhance forecasting and planning

Executives will draw on AI-driven predictive analytics and scenario modeling to assess the impact of economic downturns, climate events, and disaster scenarios, enabling stronger contingency and continuity planning. AI will also help organizations improve workforce planning by identifying skills gaps and staffing needs.

© 2026 ServiceNow, Inc. All Rights Reserved.

Appendix

Survey demographics

1,000 respondents

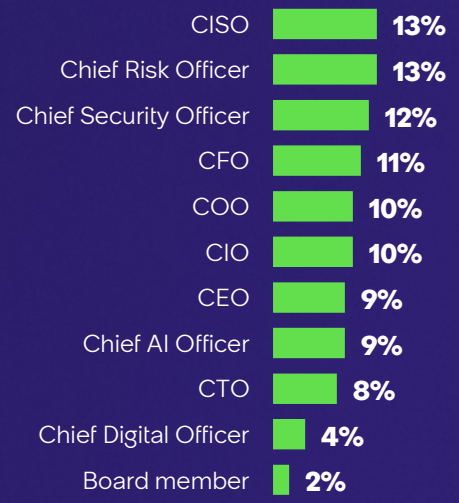
11 countries

11 industries

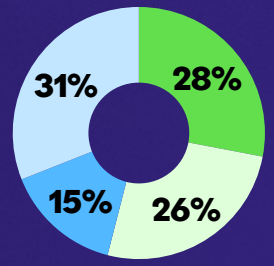
Industries

- Retail
- Financial Services
- Life sciences
- Consumer goods
- Government
- Technology
- Telecoms
- Nonprofit
- Insurance
- Healthcare
- Automotive

By title



By revenue



- Less than $1B
- $1-4.99B
- $5-9.99B
- $10B or more

Authors and contributors

Authors

Ben de Bont

Chief Information Security Officer
ServiceNow

René Stranghoner

Head of Thought Leadership Research
ServiceNow

David James

Senior Manager, PSM, Market Strategy
ServiceNow

Lou Celi

CEO
ThoughtLab

Acknowledgements

A special thanks to Monika Parashar, senior campaign manager, integrated marketing, Jessica Buckley, head of brand content, Sheila Dowd, director of thought leadership editorial, Marissa Amendolia Finn, director of brand content experience, and Emma Kieckhafer, director of social media.

Thank you to all the ServiceNow colleagues who helped bring this research to life, especially Tim Catts, Abi Hobson, Sheryl Domingue, Zoe Gaylard, and Mary Silverstein.

This report was produced in collaboration with ThoughtLab

ThoughtLab is an innovative thought leadership and economic research firm providing fresh ideas and evidence-based analysis to help business and government leaders cope with transformative change.

© 2026 ServiceNow, Inc. All Rights Reserved.

servicenow

ServiceNow (NYSE: NOW) is the AI control tower for business reinvention. The ServiceNow AI Platform integrates with any cloud, any model, and any data source to orchestrate how work flows across the enterprise. By unifying legacy systems, departmental tools, cloud applications, and AI agents, ServiceNow provides a single pane of glass that connects intelligence to execution across every corner of business. With more than 75 billion workflows running on the platform each year, ServiceNow helps organizations turn fragmented operations into coordinated, autonomous workflows that deliver measurable results. Learn how ServiceNow puts AI to work for people at www.servicenow.com

ThoughtLab is an innovative thought leadership and economic research firm providing fresh ideas and evidence-based analysis to help business and government leaders cope with transformative change. We specialize in analyzing the impact of technological, economic, and demographic shifts on industries, cities, and companies.

To learn more about ThoughtLab, visit www.thoughtlabgroup.com.