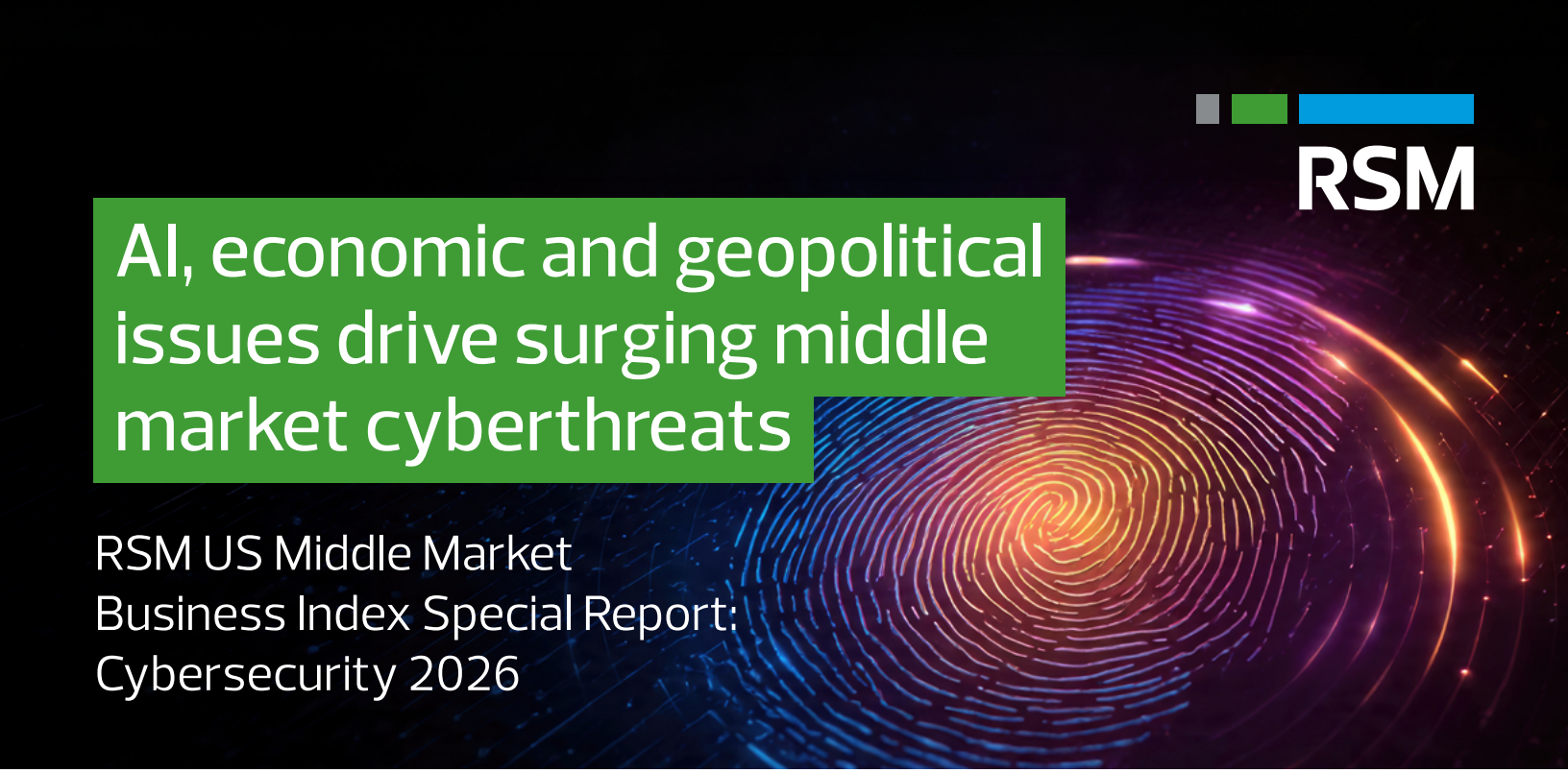


AI, economic and geopolitical issues drive surging middle market cyberthreats

RSM US Middle Market Business Index Special Report: Cybersecurity 2026

Inside the report:

The MMBI survey aggregated the responses of 501 U.S. and 101 Canadian middle market executives across a variety of industries.

Geopolitical and economic uncertainty and rapid AI adoption elevate cyber risks

Emerging threats create challenging risk environment for the middle market

Key takeaways

18% of middle market executives surveyed report suffering a data breach in the last year.

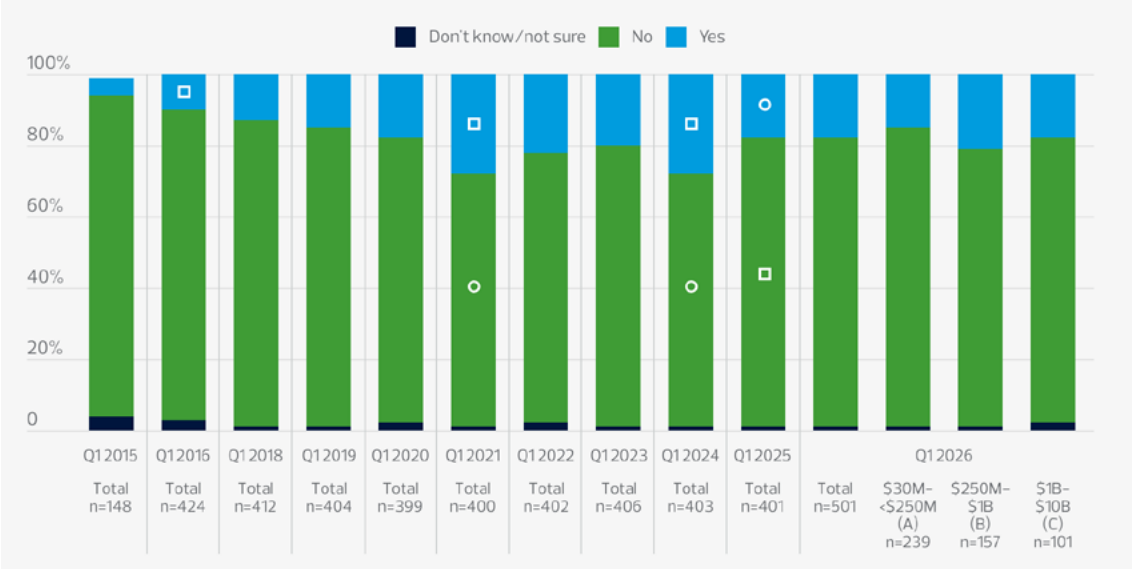
Middle market companies are at high risk because of valuable assets and uneven security controls.

Emerging threats, mainly attributed to AI, will pose significant challenges moving forward.

The middle market is navigating a confluence of events that have introduced complex, persistent cybersecurity challenges. The rapid escalation of artificial intelligence usage and threats, combined with continued economic and geopolitical concerns, is challenging risk management strategies to keep pace.

The Q1 2026 RSM US Middle Market Business Index survey, conducted from Jan. 6 to Jan. 30 on behalf of RSM by The Harris Poll, drew responses on cybersecurity from executives at 501 U.S. middle market companies across a variety of industries. The RSM Canada middle market survey was conducted from Feb. 9 to Feb. 20, interviewing 101 Canadian executives. The resulting data provides insights on cybersecurity in the middle market overall, as well as in smaller ($30 million to less than $250 million in revenue), midsize ($250 million to $1 billion in revenue) and larger ($1 billion to less than $10 billion in revenue) middle market organizations. The survey responses revealed large gaps between the groups, with smaller firms appearing to lag their larger counterparts in cybersecurity budgets and staffing, as well as in implementing AI governance practices.

Experienced a data breach in the last year*



Source: RSM US Middle Market Business Index, Q1 2026
Square/Circle = Significantly higher/lower than previous quarter, respectively, at .05 level of significance

* Base = total sample
Q1'15 base shown is total weighted base

The Canadian perspective: A quarter of Canadian executives surveyed indicated they experienced a data breach in the last year.

For the second straight year, nearly 1 in 5 (18%) middle market executives polled said their organizations experienced a data breach in the previous 12 months. Midsize companies were the most likely to have experienced a breach (21%), while smaller companies were the least likely (16%).

Middle market companies are increasingly targeted because they represent high-value environments with uneven security maturity. Organizations that prioritize identity security, visibility and vendor risk management significantly reduce breach probability.

Even with the elevated threat environment, middle market executives almost universally feel optimistic about their existing control environment. In fact, 96% of survey respondents are confident in their current security measures, nearly identical to last year's data.

However, "confidence isn't the same as preparedness," says Rich Servillas, a director at RSM US LLP. "I see a lot of gaps in incident response engagements with organizations that have good tooling but no rehearsed decisions or framework."

Despite the overwhelming level of confidence among respondents, RSM risk professionals caution companies about a new level of threats—mainly attributed to expanding AI use—that will pose significant challenges moving forward but have yet to be addressed by companies of all sizes.

"Confidence isn't the same as preparedness. I see a lot of gaps in incident response engagements with organizations that have good tooling but no rehearsed decisions or framework."

Rich Servillas, Director, RSM US LLP

AI and cybersecurity: The double-edged sword

The rapid evolution of AI introduces heightened cyber risks across several dimensions. AI's promise of increased efficiency and insight is enticing, but companies often move too quickly without effective governance in place. In addition, if individual users or teams test or use unapproved or unvetted AI and generative AI solutions, shadow AI can emerge within the organization. Both scenarios can quickly result in the exposure or loss of sensitive data.

"Organizations are constantly evaluating ways to do more with less, and the move to AI-enabled solutions is occurring very rapidly," says RSM US Principal Daniel Gabriel. "But most companies don't yet know where they want to be or what it means to get there. That acceleration opens up a lot of risk or potential avenues of risk."

RSM US Principal Steve Kane stresses how quickly shadow IT can spread. "You can only manage what you can see, and companies often don't realize that they have their own shadow IT—or they just turn a blind eye to it, and do not have the proper controls in place to manage or mitigate the challenges it brings," he says. "Meanwhile, many of their employees are using public AI tools to ask questions about how to perform certain tasks and using customer data. That's potentially instant data loss, because now that's in somebody else's cloud or somebody else's computer that you don't know."

Middle market companies must get their arms around AI deployment, even as the broader market has yet to settle on a clear approach. And middle market companies face that challenge with fewer resources at their disposal.

On the bright side, cybersecurity firms and teams are becoming more adept at leveraging AI, and more functionality is now built into security products to increase protection capabilities. AI enables the middle market to take some security measures that were previously out of reach by leveraging tools with built-in AI, essentially extending their workforce without adding personnel.

"Organizations are constantly evaluating ways to do more with less, and the move to AI-enabled solutions is occurring very rapidly. But most companies don't yet know where they want to be or what it means to get there. That acceleration opens up a lot of risk or potential avenues of risk."

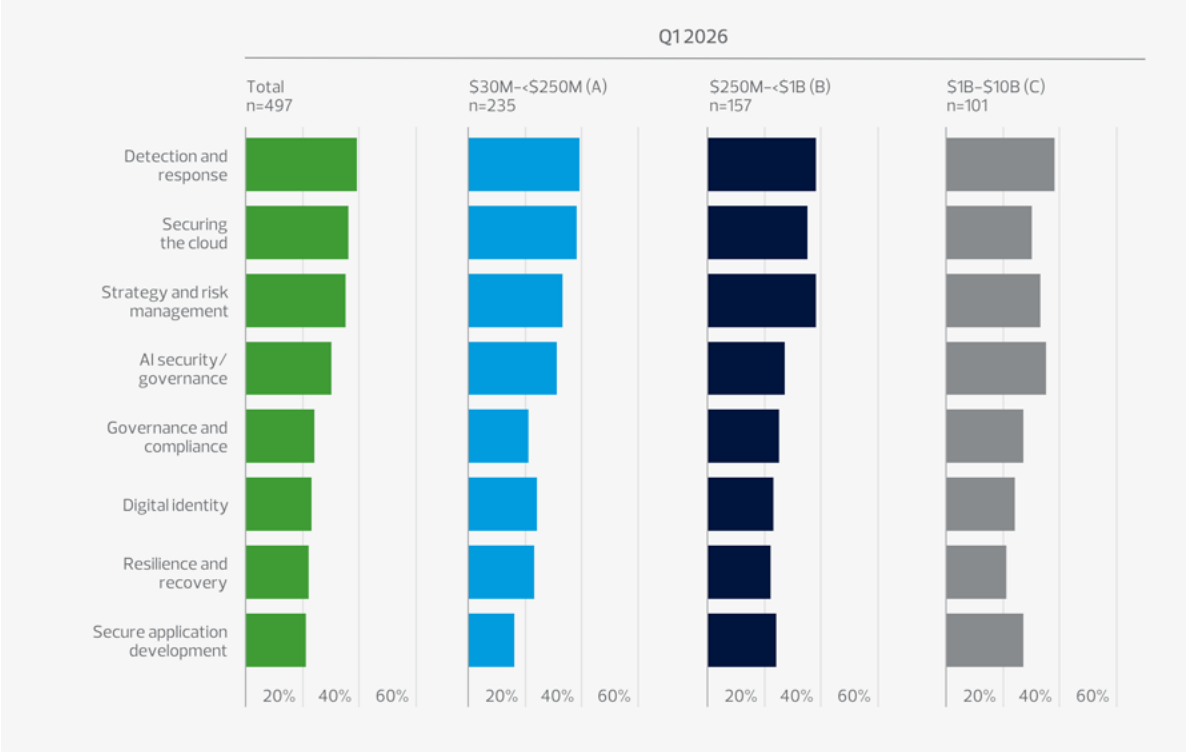
Daniel Gabriel, Principal, RSM US LLP

The identity challenge increases

In addition to AI deployment risks, the cyberthreat landscape for middle market companies is elevated because AI makes sophisticated attacks easier to launch. Campaigns that previously required an exceptionally gifted threat actor and months to develop can now be orchestrated at scale by a relative novice with AI assistance.

The growing use of AI underscores the need for critical security features in the middle market: identity and access, privileged access, the controlling of sensitive data and the assignment of authorizations.

Top 3 information cybersecurity and data privacy initiatives being undertaken for fiscal year*



Source: RSM US Middle Market Business Index, Q1 2026

* Base = total sample

MMBI survey respondents reported focusing their resources mainly on detection and response (39%), securing the cloud (36%), and strategy and risk management (35%). Digital identity, prioritized by only 23% of respondents, represents a significant missed opportunity to focus on what human and nonhuman users can access rather than where they are connecting from.

"Identity is at the center of information compromises," says RSM US Principal Alden Hutchison. "Most threat actors don't break in. They log in. When identity controls and permissions are weak, attackers don't need exploits. As organizations adopt AI, those same gaps scale faster, because AI will act on any access it's given, intended or not."

Identity is the focal point of securing AI, establishing rights and defining what it is authorized to do. However, companies often debate how to structure authorizations: Should AI tools have authorizations all the time and their own specific identity, or should they inherit the identity of the user? Companies have dealt with these questions for human identities in the past, but their importance is elevated because of the rapid growth of nonhuman identities.

Gabriel emphasizes the identity challenges organizations face in an uncertain environment. "It's just a very difficult time, mostly because companies don't necessarily know how to respond," he says. "Companies have some basic guidelines on things they need to do fundamentally, but nobody truly knows what the future of AI holds."

"Most threat actors don't break in. They log in. When identity controls and permissions are weak, attackers don't need exploits. As organizations adopt AI, those same gaps scale faster, because AI will act on any access it's given, intended or not."

Alden Hutchison, Principal, RSM US LLP

Increased pressure on cybersecurity budgets

Amid ongoing economic uncertainty, fewer middle market companies are increasing cybersecurity investments, even in the extremely challenging threat environment. In the MMBI survey, 81% of respondents said they plan to increase their cybersecurity budget, a decrease from 91% last year. As companies navigate tariff expenses, rising energy costs and business complexity related to geopolitical conflicts on multiple fronts, many are reevaluating their spending to address potential cybersecurity threats.

"Rising costs have caused organizations to make tough decisions," says Gabriel. "Understandably, when things get tight, companies tend to pivot money to what keeps the lights on and generates revenue for the organization. But companies cannot lose focus on cybersecurity, because this a time when threat actors are arguably more active and dangerous than they have ever been."

Companies balance risk and budget pressure as cyber spend and structures shift

Cybersecurity leadership and spending undergo change amid evolving challenges

Key takeaways

81% of middle market survey respondents plan to increase cybersecurity spending.

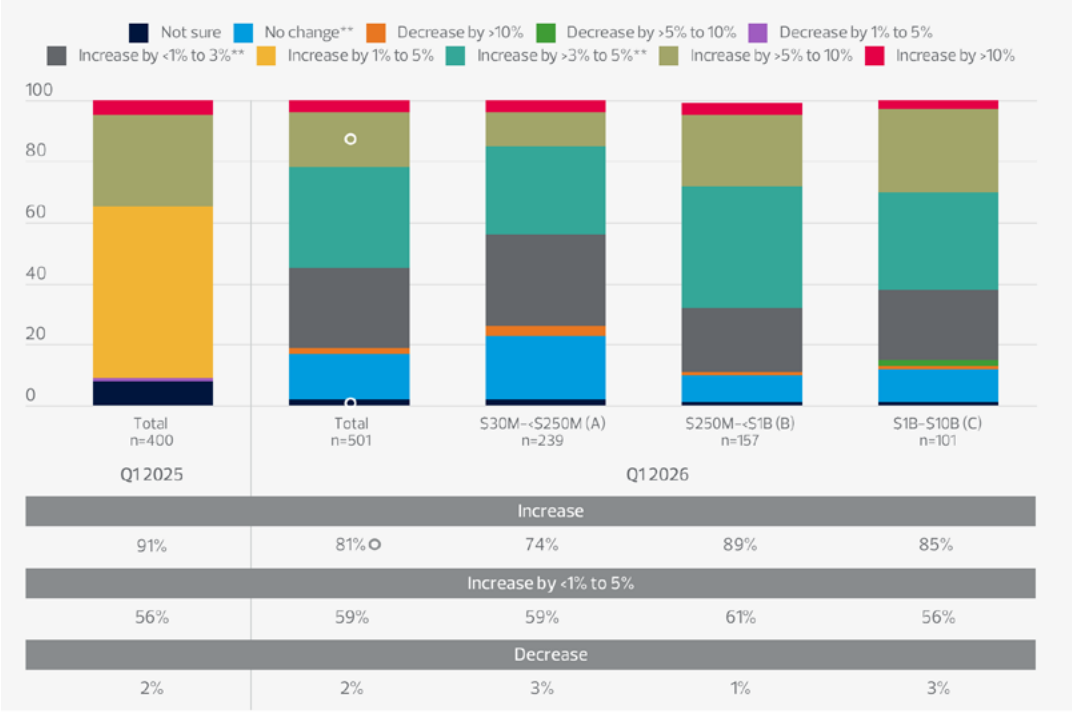
Cyber budgets in the middle market are most often located under the chief technology officer.

Cloud security management and security awareness training are top targets for outsourcing.

As the cybersecurity environment continues to evolve and new threats emerge, Q1 2026 RSM US Middle Market Business Index survey data shows that the security approaches of many middle market companies are also shifting significantly. Financial pressures are leading to structural changes in many cybersecurity departments, but companies cannot afford to lose sight of persistent risks.

In the survey, 81% of respondents said they plan to increase their cybersecurity spending in the coming year, a drop from 91% last year. With ongoing economic uncertainty, many middle market companies are taking a more cautious approach to cybersecurity spending.

Expected cybersecurity budget change*



Source: RSM US Middle Market Business Index, Q1 2026
**New response options added in Q1'26
Square/Circle = Significantly higher/lower than previous quarter, respectively, at .05 level of significance

* Base = total sample

The Canadian perspective: 93% of Canadian firms plan to increase their cybersecurity budget in the coming year, compared to 81% of U.S. companies.

When revenue visibility is unclear, cybersecurity decisions get harder, not easier," says RSM US LLP Principal Alden Hutchison. "That's where many middle market companies struggle. Pulling back indiscriminately increases risk. The smarter move is prioritization. Spend that reduces material exposure stays. Everything else gets questioned."

Survey results showed that for U.S. respondents, the cybersecurity budget is now most often located under the chief technology officer (43%), followed by the chief financial officer (37%) and chief information security officer (34%). In last year's survey, the CEO/president/owner controlled the cybersecurity budget most often, along with the CFO (both 42%); this year, the CEO/president/owner role controls the budget for only 25% of companies.

The responsibility for guiding cybersecurity planning and execution has also undergone a shift this year. Asked who oversees cybersecurity and related decision making, the top responses were a dedicated CISO or equivalent role (30%); a chief information officer or another executive-level leader (24%); and the IT department, without a dedicated cybersecurity leadership position (20%). The IT department was listed as the responsible party most often in last year's data (25%), followed by a dedicated CISO (22%).

"When revenue visibility is unclear, cybersecurity decisions get harder, not easier. That's where many middle market companies struggle. Pulling back indiscriminately increases risk. The smarter move is prioritization. Spend that reduces material exposure stays. Everything else gets questioned."

Alden Hutchison, Principal, RSM US LLP

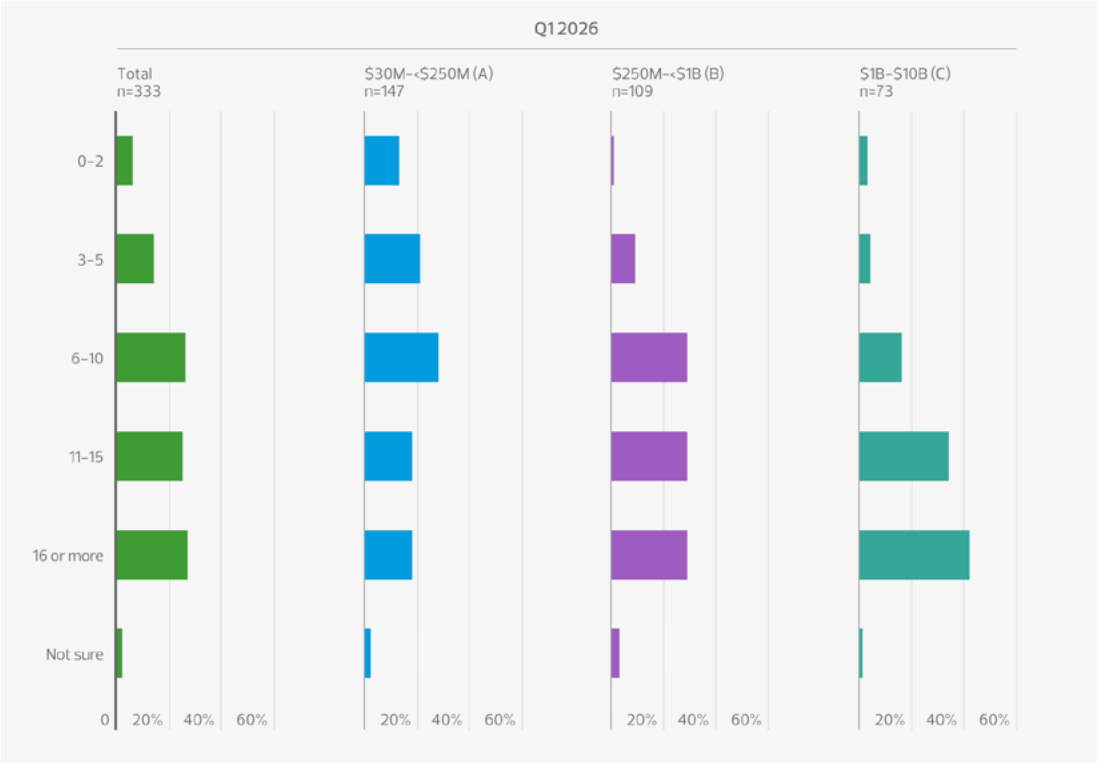
Building an effective cybersecurity workforce

From a staffing perspective, 52% of middle market respondents reported having more than 11 employees dedicated to data security and data privacy, 46% have 10 or fewer and 20% have less than five. Not surprisingly, larger middle market companies have more dedicated internal staff, with the largest share (42%) indicating they have 16 or more employees. On the other hand, most respondents from smaller middle market companies have five or fewer (34%).

"Larger organizations are on the build side of the build versus buy equation for cybersecurity departments," says RSM US Principal Steve Kane. "A, they can afford it, and B, they often have differing business needs that require keeping personnel in-house. Many need customized approaches to processes that are more difficult for managed service providers to provide. However, all organizations have limited cyber budgets and should take a hard look at the outcomes that are a priority. Many times, managed services can provide the outcomes clients really need at a fraction of the cost of building it yourself."

Board involvement in cybersecurity at larger companies typically translates to more internal personnel. "As you move upmarket, especially in public companies, there's already board awareness around cybersecurity," RSM US Principal Autumn Hurley says. "The board's responsibility is to ensure a strong cybersecurity program is in place because it can affect the bottom line. In addition, cybersecurity is making its way into enterprise risk programs, so leaders are treating it as an enterprise priority."

Number of employees dedicated to data security and data privacy*

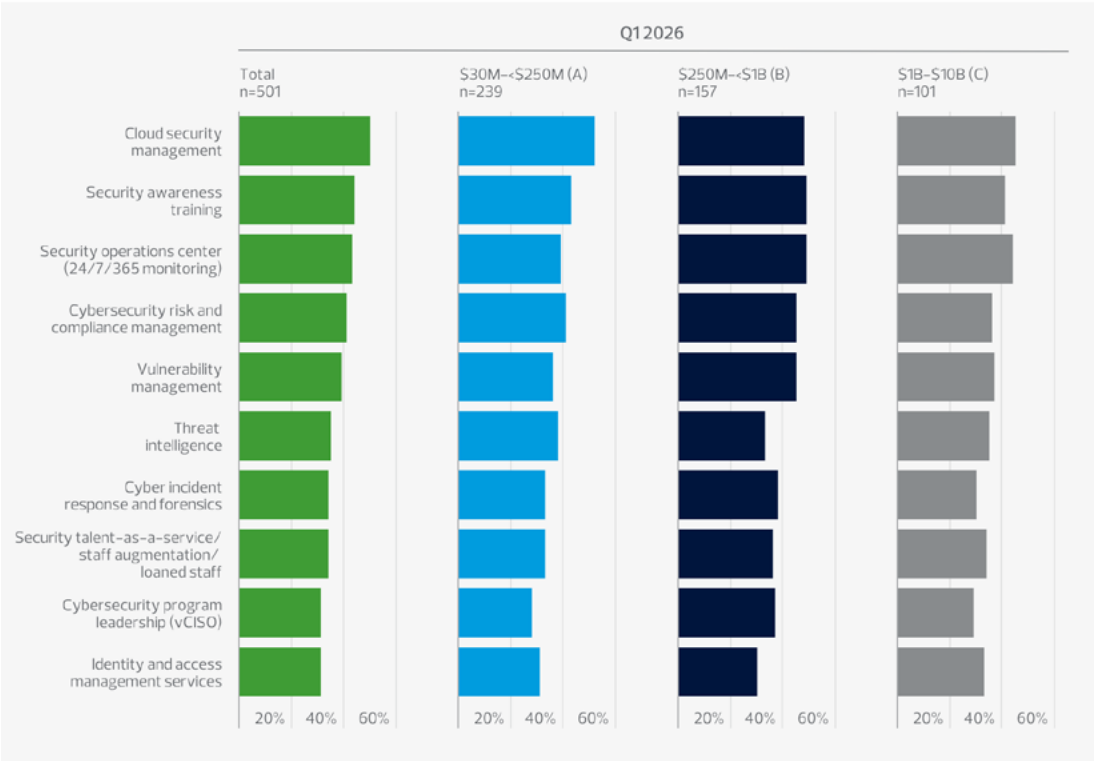


Source: RSM US Middle Market Business Index, Q1 2026

* Base = Has CISO, IT department or cross-functional committee responsible for cybersecurity strategy and decision making

Regardless of the size of internal departments, many middle market companies continue to rely on outsourcing for key cybersecurity functions, especially for specialized tasks. Respondents indicated that the leading cybersecurity functions currently outsourced are cloud security management (50%), security awareness training (44%), security operations center (43%), and cybersecurity risk and compliance management (41%).

Cybersecurity functions currently outsourced*



Source: RSM US Middle Market Business Index, Q1 2026

* Base = total sample

"Cloud security management is definitely something that requires a high level of expertise," RSM US Principal Autumn Hurley says. "Cloud security engineering is a very specialized skill set, and a lot of organizations don't feel comfortable with it or they feel that they don't have the talent internally to support that."

"The cybersecurity workforce of the future is currently under construction, and companies need to consider how to build their departments moving forward. This includes how they staff and how they determine the right balance of insourcing versus outsourcing, and reliance on humans versus nonhuman resources. That's a big pivot."

Daniel Gabriel, Principal, RSM US LLP

As with many other key business processes, AI is affecting how middle market companies leverage service providers. In many ways, AI is an evolution of the service provider, augmenting internal teams as it becomes more stable, more directed and more reliable. Service providers are reinventing what they deliver and are still better equipped to leverage tools underpinned with AI than internal personnel in most cases. But many organizations are reconsidering what they outsource to providers versus what they do in-house, utilizing products and essentially outsourcing activities to nonhuman entities in a trusted fashion.

"The cybersecurity workforce of the future is currently under construction, and companies need to consider how to build their departments moving forward," says RSM US Principal Daniel Gabriel. "This includes how they staff and how they determine the right balance of insourcing versus outsourcing, and reliance on humans versus nonhuman resources. That's a big pivot."

Middle market remains vulnerable to cyberattacks, but controls improve

Many breach threats remain consistent, but AI escalates risks

Key takeaways

96% of middle market executives surveyed are confident in current measures to safeguard data.

24% of survey respondents experienced at least one ransomware attack or demand in the last year.

Endpoint detection and response and managed detection and response are beneficial risk strategies.

Given the prevalence of cybersecurity risks, middle market companies generally understand that a data breach is likely at some point. With that in mind, some with mature security programs are shifting to an "assume compromise" perspective, which presumes a threat actor is already present. In a consistently challenging threat environment, leadership needs to continue focusing on putting effective controls in place to shield their companies and minimize risks as much as possible.

Despite the growing complexity of effective cybersecurity management, 96% of middle market executives in the Q1 2026 RSM US Middle Market Business Index survey reported that they are either very or somewhat confident in their current measures to safeguard data, similar to last year.

Risks and vulnerabilities are also largely unchanged. "Many issues are pretty consistent from what we saw last year," says Rich Servillas, a director at RSM US LLP. "Exposed edge devices are the dominant initial access vector. Many events are also attributed to gaps in a victim's firewall, as well as virtual private network (VPN) and multifactor authentication (MFA) issues. It's a lot of low-hanging fruit."

Many of the industries targeted by threat actors have stayed consistent as well, with financial services, health care and manufacturing entities at high risk.

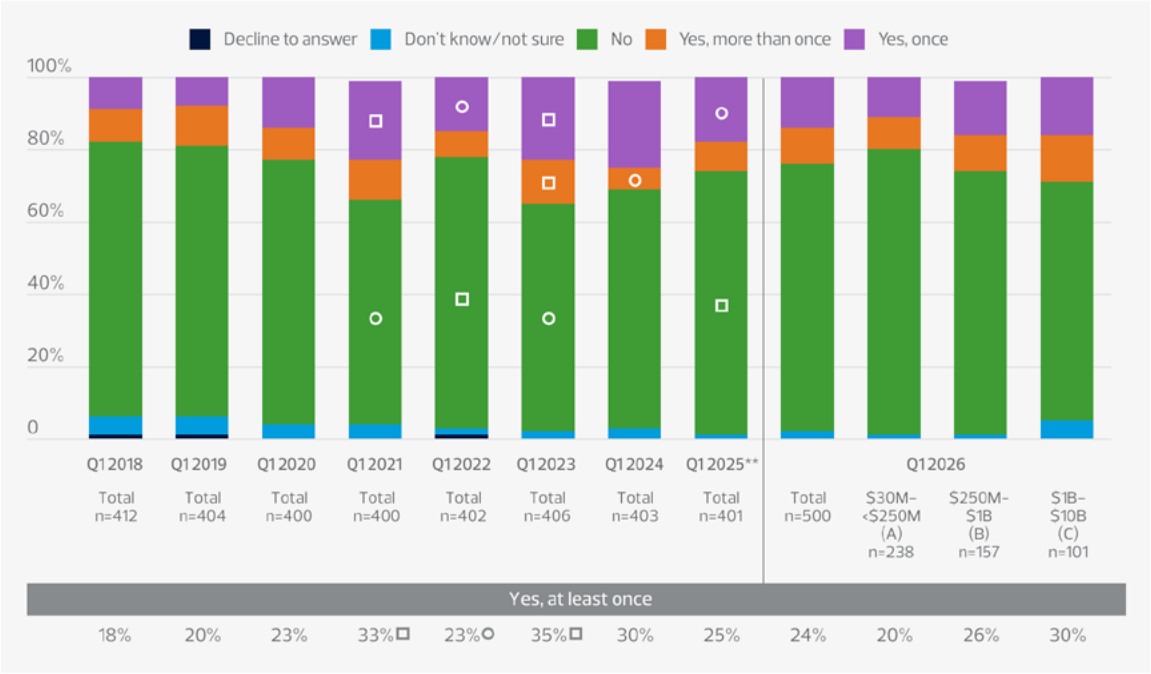
"Health care organizations, as well as school districts, municipalities and regional manufacturers all share the same profile," Servillas says. "High operational pressure, limited budgets and low tolerance for downtime. Threat actors have figured out that leverage, not sophistication, is what drives payment. Municipal entities and K-12 schools have become priority targets for lone wolf and mid-tier affiliate operators because they combine operational pressure with typically low security maturity."

Ransomware represents a continued threat to operations and sustainability. In the Q1 2026 RSM US MMBI survey, 24% of middle market companies reported experiencing at least one ransomware attack or demand in the last 12 months, similar to last year. Larger companies, with more attractive data and financial assets, were prime targets for criminals: 30% of respondents experienced at least one attack or attempt compared to 20% of smaller counterparts.

"With ransomware, I think about what actually causes people to pay," says Servillas. "A few years ago, it was almost always about backups, because victims often didn't have good redundancy in place, so they had to pay to get their data back and stay in business. That's shifted. Now more often they're paying to keep stolen data from being leaked. It's not advised to pay, but when the data is sensitive enough, the decision gets harder."

Like other cyberthreats, ransomware attacks have intensified with the use of AI. Enhanced automation has increased the ease and quality of business email compromise attacks, while also enhancing spear phishing and vishing attacks, where an attacker may pretend to be a help desk employee, for example.

Experienced a ransomware attack or demand during the last 12 months*



Source: RSM US Middle Market Business Index, Q1 2026
** "Decline to answer" omitted from total answering base starting in Q1'25
Square/Circle = Significantly higher/lower than previous quarter, respectively, at .05 level of significance

* Base = total sample

"The ransomware-as-a-service era is fading, and more of what we're responding to is lone-wolf operators. AI is what's making them dangerous. It's closing the gap between a sophisticated attacker and someone who wouldn't have been a threat 18 months ago."

Rich Servillas, Director, RSM US LLP

"We're seeing early signs of AI in how threat actors communicate, with cleaner language, faster responses and more consistent tone," says Servillas. "The bigger shift is who's using it. The ransomware-as-a-service era is fading, and more of what we're responding to is lone-wolf operators. AI is what's making them dangerous. It's closing the gap between a sophisticated attacker and someone who wouldn't have been a threat 18 months ago. We're not yet seeing attacks run entirely by AI, but that's where this is trending."

"However, Servillas sees some promising signals from control strategies in the middle market. "A lot of companies are making meaningful progress," he says. "The conversations are shifting from 'We are completely down,' to 'We believe we caught the activity while it was still unfolding and were able to contain it.'"

"Endpoint detection and response (EDR) maturity has genuinely improved outcomes, and we are seeing more and more incidents getting contained at the initial access or lateral movement phase, prior to encryption," Servillas continues. "In addition, managed detection and response services are helping accelerate middle market wins. We do see a lot of organizations that don't have 24/7 in-house security operations center coverage—but it's nice to see some advancements driving forensic and breach costs down."

Cybersecurity risk strategies in the middle market evolve as new risks emerge

The attack surface is growing, and protective strategies must adapt accordingly

Key takeaways

40% of survey respondents use a formal risk management framework to assess and manage cyber risks.

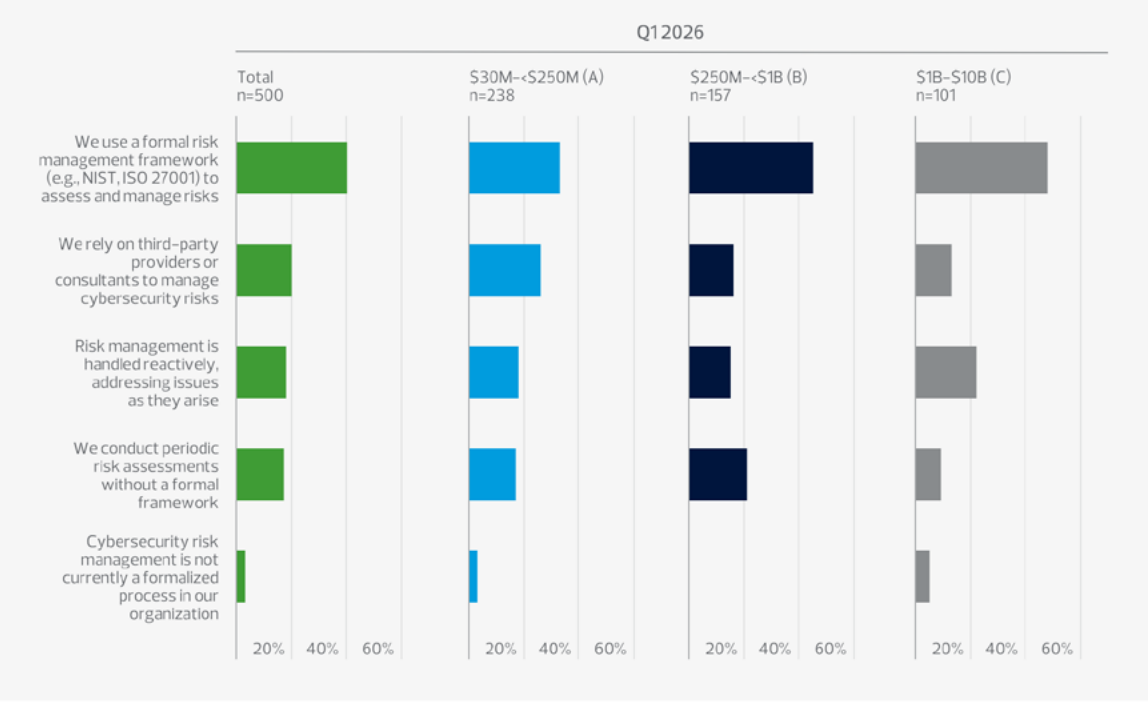
75% of middle market executives report carrying a cyber insurance policy.

Cyber insurance is evolving, but it remains important with the potential severity of attacks.

A comprehensive risk management strategy is the most critical element of an effective cybersecurity stance. As the attack surface continues to grow, companies must proactively implement leading strategies to address emerging risks and implement controls that align with overall business goals.

For example, many middle market companies are shifting from point-in-time governance strategies that can fail to address modern risks to a more dynamic continuous monitoring and autonomous risk management approach. These leading organizations are leveraging tool sets to aggregate data from various sources and gain a more holistic and real-time perspective on their cyber hygiene.

Approach to identification and management of cybersecurity risks*



Source: RSM US Middle Market Business Index, Q1 2026

* Base = total sample

The Canadian perspective: Canadian survey respondents also reported using a formal risk management framework as their leading approach to identification and management of cybersecurity risks, but at a higher rate than U.S. companies (53% vs. 40%).

"In the past, companies had several disparate systems—perhaps identity and access management in one system and third-party risk management in another," says RSM US LLP Director Amy Feldman. "With continuous monitoring, we are now able to leverage the data from those systems in a single location with real-time insights that draw larger conclusions around the broader risk posture instead of monthly or quarterly reports that don't align insights with risk indicators."

In the Q1 2026 RSM US Middle Market Business Index survey, the use of a formal risk management framework to assess and manage risks was the leading approach to identifying and managing cybersecurity risks, reported by 40% of respondents compared to 24% last year. Relying on third-party providers or consultants to manage cybersecurity risks ranked second (20%), followed by handling risk management reactively, addressing issues as they arise (18%).

"What we're seeing is that people in a risk management or cybersecurity role had to start putting more formal frameworks in place to measure success and show progress to boards and audit committees," says Feldman. "So, I think a lot of the uptick in leveraging frameworks is because of pressures that probably started externally following highly publicized incidents but were subsequently pushed down from senior leadership."

"In the past, companies had several disparate systems—perhaps identity and access management in one system and third-party risk management in another. With continuous monitoring, we are now able to leverage the data from those systems in a single location with real-time insights that draw larger conclusions around the broader risk posture instead of monthly or quarterly reports that don't align insights with risk indicators."

Amy Feldman, Director, RSM US LLP

RSM US Principal Alden Hutchison also highlights the importance of leveraging an established framework to guide cybersecurity decisions. "Organizations are recognizing that you can't manage cyber risk without a common measurement framework," he says. "NIST and ISO give leaders a consistent way to assess maturity, prioritize investment and demonstrate progress to boards, regulators and audit committees."

Cyber insurance remains a popular tool in the middle market to protect data and quickly recover if a cyberattack occurs. However, policies have undergone several changes in recent years to reflect the evolving risk environment.

In the MMBI survey, 75% of respondents reported carrying a cyber insurance policy, a drop from the record high 82% in last year's survey, but in line with the previous high of 76% two years ago.

"From a third-party risk management perspective, we're seeing a lot of clients really pushing for their vendors to have an acceptable level of coverage within their cyber liability insurance rather than checking the box to indicate they hold coverage," says Feldman. "I've seen a lot of our customers react to these requests to ensure they can keep the business, but the premiums are getting more expensive and policy coverage is getting less and less expansive."

Even with policy changes, Hutchison emphasizes the importance of cyber insurance. "The decline in cyber insurance adoption is surprising, because the risk environment hasn't improved," he says. "Attacks are increasing, incidents are more expensive, and insurance remains a critical risk-transfer mechanism. Opting out doesn't reduce exposure. It concentrates it."

As AI use advances, digital identity risks require increased attention

Identity has moved to the forefront of cybersecurity strategies in the AI age

Key takeaways

As AI threats persist, digital identity strategies must continue to improve.

49% of survey respondents have a centralized IAM system with support for MFA.

44% of middle market executives report using biometric authentication and password management.

Having a clear perspective on digital identity has never been more important for middle market companies amid growing risks from human and nonhuman identities. With AI solutions and related threats continuing to develop, identity must be a focal point of any cybersecurity risk program.

Middle market organizations are in various phases of their approach to identity, which can range from focusing on establishing initial foundational controls to reaching a mature state or tackling emerging risks.

"Identity is a continuous conversation," RSM US LLP Principal Autumn Hurley says. "Many organizations are early in their journey to building out a mature identity program. It takes a lot of thoughtful strategic planning to lay the foundation for a successful program."

Identity programs encompass both human and nonhuman identity management. Core concepts such as user lifecycle management within an organization, third-party identity governance, privileged access, secrets management, secure authentication, customer identity lifecycle management, and identity posture and visibility each require dedicated attention. Together, however, these elements form a robust and integrated capability that helps organizations manage risk while also driving operational efficiency.

"Identity is a continuous conversation. Many organizations are early in their journey to building out a mature identity program. It takes a lot of thoughtful strategic planning to lay the foundation for a successful program."

Autumn Hurley, Principal, RSM US LLP

The proliferation of AI has increased the difficulty of managing identity risks, specifically in the nonhuman identity space.

"Nonhuman identity is not a new concept," says RSM Canada Partner Omer Arshed. "This is something we've been managing for clients for over a decade. But AI has changed and added further complexity to the equation."

Before AI's explosive growth, nonhuman identity referred to service accounts, application programming interface (API) keys, Secure Shell (SSH) keys, certificates, and right tokens used by cloud or DevOps processes or app-to-app communications. That definition still stands, but the nonhuman identity risk has now expanded to the world of agentic AI.

"Now, you have digital workers, digital bots and digital agents that are running processes that humans or applications previously performed," says Arshed. "To do that, they not only need the level of authorization and privilege to get access to production resources to accomplish those tasks but also must be identified and mapped to business process owners, application owners, platform owners and other functions important to the organization. Agents that perform actions and interactions in the environment must be led by zero-trust principles, be auditable, produce required logs and be monitored."

"Nonhuman identity is not a new concept. This is something we've been managing for clients for over a decade. But AI has changed and added further complexity to the equation for nonhuman identity."

Omer Arshed, Partner, RSM Canada

Growth can also elevate identity concerns. For example, when companies conduct mergers or acquisitions, combined entities often end up with conflicting, outdated or multiple sets of identity controls that need to be modernized and updated or merged to reduce potential risks.

In the Q1 2026 RSM US Middle Market Business Index survey, 49% of middle market respondents said their primary method for managing digital identity and securing systems access is a centralized identity and access management (IAM) system with support for MFA.

This finding was followed closely by biometric authentication (44%)—which can include fingerprint recognition, facial recognition, iris or retinal scans, voice recognition, or palm or vein pattern recognition—and password management (44%), which relies on strict policies such as regular updates and complexity requirements but with no IAM system in place.

Although middle market organizations are addressing key secure authentication and identity management risks, complexities are increasing, and additional controls are required to manage identity risk.

Traditionally, the middle market has lagged in many foundational areas related to identity. However, RSM US Principal Alden Hutchison sees some real opportunities for middle market companies to gain better control over identity risks.

"Modern identity controls have matured to the point where they're more accessible for the middle market," he says. "Companies can now deploy enterprise-grade identity capabilities at a reasonable cost, whether through modern platforms or managed services that deliver outcomes without the overhead."

Methods used to manage digital identities and secure systems access*

Source: RSM US Middle Market Business Index, Q1 2026

* Base = total sample

The Canadian perspective: Canadian survey respondents also reported using a centralized IAM system with support for MFA as their leading method to manage digital identity and secure system access, but at a higher rate than U.S. companies (62% vs. 49%).

Identity controls have rapidly evolved from password and multifactor strategies to more sophisticated facial, biometric and passwordless options.

"The shift to biometric and passwordless identity controls has changed adoption dynamics," says Hutchison. "These options reduce user friction and make it easier for middle market companies to implement stronger identity strategies at scale."

"Modern identity controls have matured to the point where they're more accessible for the middle market. Companies can now deploy enterprise-grade identity capabilities at a reasonable cost, whether through modern platforms or managed services that deliver outcomes without the overhead."

Alden Hutchison, Principal, RSM US LLP

Accelerating AI governance: Taking a stronger stance on surging AI risks

Secure AI adoption is pivotal for mitigating AI threats and optimizing value

Key takeaways

Many organizations are still working to establish effective AI governance.

51% of survey respondents conduct staff training on responsible AI usage and development.

46% utilize data governance policies to support data quality and privacy for use in AI models.

AI has rapidly advanced to permeate every corner of the operating environment for middle market companies. Leveraging AI tools and strategies is a must to generate the efficiency, insight and productivity necessary to succeed, but companies must integrate effective governance to mitigate persistent risks.

As new use cases emerge and solutions evolve, middle market companies are continually adjusting AI strategies to transform key processes. Users are understandably excited to take advantage of new technology, learn new skills and contribute to business growth. However, as in many cases, humans are often the weakest link from a security perspective, and many companies are encountering significant shadow AI risks from the use of unauthorized tools.

All too often, users test or pilot AI tools lacking the company's established guardrails, without proper tracking and governance. This scenario creates a host of issues, from data leakage to zombie accounts where users set up a test account and upload sensitive information that the company doesn't know about and wasn't monitoring for.

"AI introduces two reinforcing risks," says RSM US LLP Principal Alden Hutchison. "Internal users expose data through shadow AI, and attackers exploit AI once identity is compromised. In both cases, lack of governance turns AI into an accelerant, not the root cause."

In addition, AI solutions are being integrated within many existing business technology tools companies already leverage, introducing additional threat vectors.

"You can assume that these AI solutions are well tested and protected," says RSM US Principal Daniel Gabriel. "But still, what information do you want to provide to third-party companies? You must rethink how you are engaging with these organizations."

"AI introduces two reinforcing risks. Internal users expose data through shadow AI, and attackers exploit AI once identity is compromised. In both cases, lack of governance turns AI into an accelerant, not the root cause."

Alden Hutchison, Principal, RSM US LLP

Protecting the ghost in the machine

As a nonhuman decision-making engine within the business, AI has been described as a ghost in the machine—one requiring protection through the following measures:

- **Observe** all AI usage; understand AI components and the machine learning/AI bill of materials; and inventory data provenance.
- **Assess** hidden AI vulnerabilities, operational impact and autonomous agents.
- **Control** data leakage and inaccurate/false insights to ground retrieval-augmented generation and privilege escalation.
- **Monitor** and remediate performance erosion, response lag and accountability gaps.

From an AI governance perspective, 51% of respondents in the Q1 2026 RSM US Middle Market Business Index survey reported conducting staff training on responsible AI usage and development, making it the most widely implemented control, up from 36% last year. Close behind were:

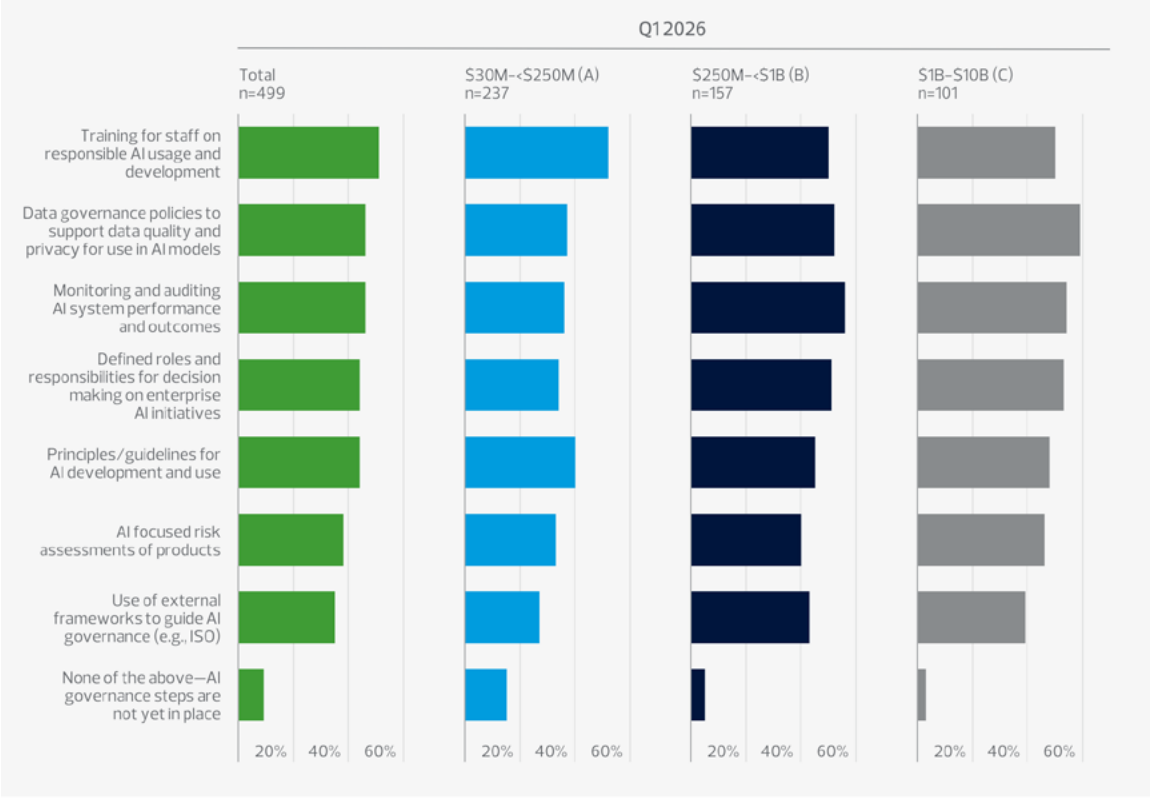
46%
have data governance policies to support data quality and privacy for use in AI models

46%
monitor and audit AI system performance and outcomes

44%
have defined roles and responsibilities for enterprise AI decision making

44%
have established principles/guideline for AI development and use

AI governance practices*



Source: RSM US Middle Market Business Index, Q1 2026

* Base = total sample

The Canadian perspective: The leading AI governance practice among Canadian survey respondents was data governance policies to support data quality and privacy for use in AI models (60%), followed by training for staff on responsible AI usage and development (54%).

The survey results were a direct reflection of the growing importance of AI in the middle market, as each answer showed increases from last year and the top five options showing double-digit growth. However, the use of external frameworks to guide AI governance may be a missed opportunity. While more than a third of respondents reported using AI governance frameworks (35%), the option ranked seventh among respondents and tied for the smallest amount of growth from last year.

"Many organizations are still trying to figure out what effective AI governance is," says RSM US Principal John Huyette. "Therefore, I am surprised that more are not mapping their AI strategies to some of the existing frameworks, such NIST RMF, ISO or responsible AI guidelines from Microsoft and other leading solution providers. To protect the ghost in the machine, adopting a governance framework is certainly a step in the right direction."

Gabriel stresses the value of AI governance and the potential for companies to make positive change in their AI strategies. "Organizations are now at a pivotal moment where they have the opportunity to do things right and make the secure adoption of AI a priority," he says. "Companies can ignore it and keep doing what they are doing and play catch-up to address issues in a reactive manner, or do it correctly to put themselves in an advantageous position going forward."

"Many organizations are still trying to figure out what effective AI governance is, Therefore, I am surprised that more are not mapping their AI strategies to some of the existing frameworks, such NIST RMF, ISO or responsible AI guidelines from Microsoft and other leading solution providers. To protect the ghost in the machine, adopting a governance framework is certainly a step in the right direction."

John Huyette, Principal, RSM US LLP

Middle market cloud strategies are maturing, but may need refinement

Many companies are evaluating cloud deployments to optimize security and value

Key takeaways

The largest share of middle market companies surveyed have 21%–50% of their environment in the cloud.

43% of respondents leverage hybrid solutions that combine on-premises and cloud security.

With risks increasing, extensive due diligence is necessary when evaluating cloud options.

For many years, middle market companies have moved infrastructure and assets to the cloud to increase security and enhance process efficiency. However, while the majority of companies are using the cloud in some fashion, many may need to reevaluate strategies to maximize effectiveness and limit potential risks.

In the middle market, the pace of cloud migration has slowed because most companies have already completed their transition. During the years of rapid adoption, many took a giant leap into the cloud, but not all were completely ready or fully understood how to get the most out of the technology.

"What we're seeing right now is a pause where companies realize they need to manage their cloud strategy in a more sophisticated way to get the most out of it and limit potential risks," says RSM US LLP Director Justin Devine. "Companies might not be getting all the benefits they wanted out of the cloud, so they're slowing down to figure it out and do it right."

Q1 2026 RSM US Middle Market Business Index survey data shows how middle market companies balance assets between the cloud and on-premises environments. The greatest share of survey respondents (30%) reported having 21%–50% of their environment operating in the cloud, followed closely by those with 51%–75% in the cloud (28%). For larger middle market companies, the top result (36%) was 51%–75%, while the leading response for smaller companies (27%) was 21%–50%.

However, in many cases, splitting assets between cloud and on-premises environments without a dominant platform can present operational and risk challenges.

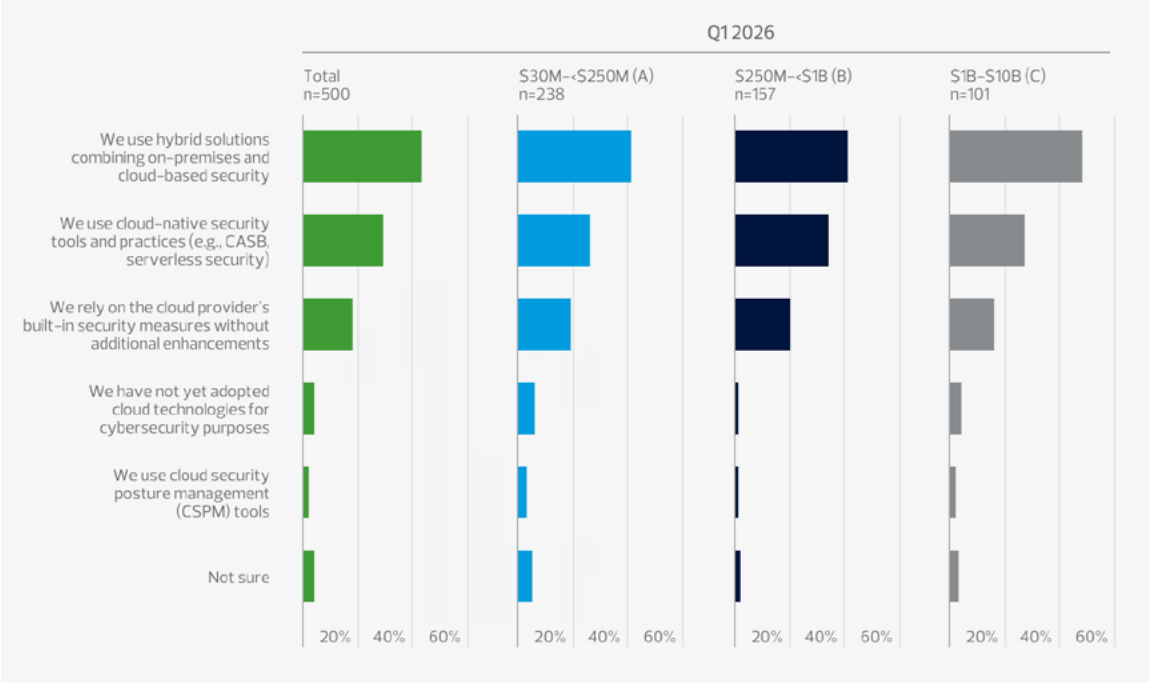
"If you have one foot in the cloud and one foot on-premises, you have to worry about both," says Devine. "You've given yourself double duty, but you likely don't have the budget and resources for that. If you're not doing one of the two well, that creates a lot of risk."

Middle market companies have a clear opportunity to commit to one platform and reduce the burden of double costs, double processing and double governance.

In the MMBI survey, respondents cited the following as the leading cloud technologies used to enhance cybersecurity efforts:

43%	29%	18%
Hybrid solutions that combine on-premises and cloud security	Cloud-native tools and practices	A cloud provider's built-in security measures without additional enhancements

Cloud technologies used to enhance cybersecurity*



Source: RSM US Middle Market Business Index, Q1 2026

* Base = total sample

In the current threat environment, many companies are concerned about the increasing number of security breaches at cloud providers, highlighting the importance of due diligence when evaluating cloud options.

"If you have one foot in the cloud and one foot on-premises, you have to worry about both. You've given yourself double duty, but you likely don't have the budget and resources for that. If you're not doing one of the two well, that creates a lot of risk."

Justin Devine, Director, RSM US LLP

"Middle market firms need to be sure that their cloud security is as good as or better than their on-premises security," says Devine. "As the number of cloud breaches rises, the cost for firms is going way up."

The costs related to cloud deployments are another major consideration for middle market companies. Cloud expenses are rising for many, with potential risk repercussions.

"Cost and security go hand in hand," says Devine. "You need to be cost conscious with cloud investments so you don't end up in a situation where you're so cost constrained that you can't do security right."

Persistent risks emphasize business continuity and incident response importance

As threats increase, limiting disruptions and sustaining operations are critical

Key takeaways

37% of middle market executives surveyed test incident response plans quarterly.

56% of respondents have implemented disaster recovery plans for critical systems.

AI is enhancing incident response, improving detection, attack warnings and containment.

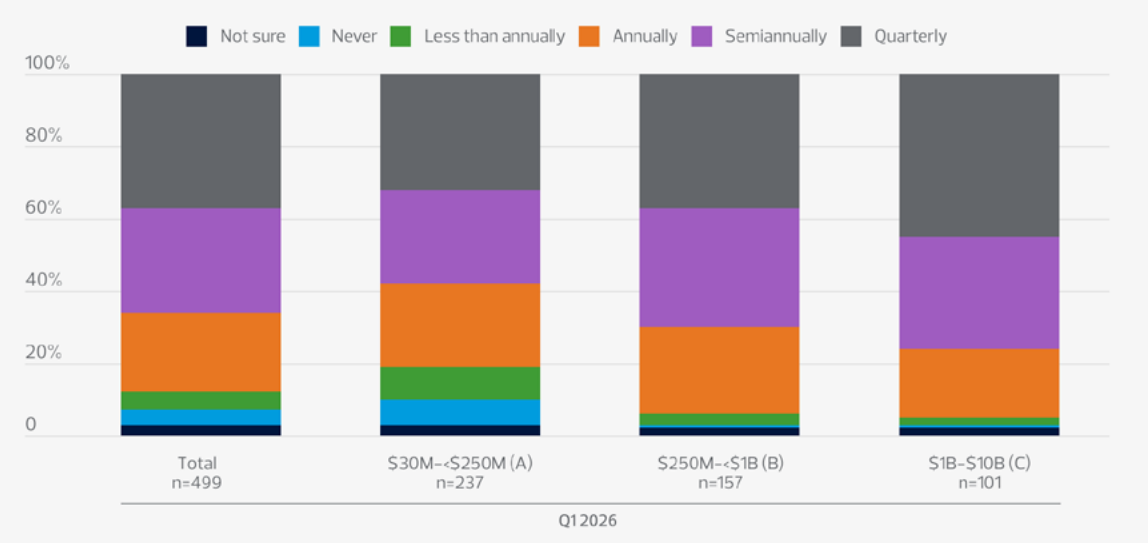
With the level of risk in the middle market, the likelihood of a cyberthreat actor finding a way into a company's environment is very high. Conducting effective business continuity and incident response planning, testing those plans, and developing decision governance will increase resilience and minimize risks.

Breaches happen, and when they do, an effective response is paramount. An incident response plan lays the groundwork for how an organization will detect, react to and recover from a cybersecurity event. It must detail roles and responsibilities, outline key procedures and establish decision rights—e.g., who can authorize a ransom payment, approve external communications, speak to regulators, etc. But for a plan to be effective, it must be regularly tested.

In the Q1 2026 RSM US Middle Market Business Index survey, quarterly testing of incident response plans was the most common practice (37%), followed by semiannual testing (29%). A bigger percentage of larger middle market companies opted for quarterly testing (45%) compared to their smaller counterparts (32%).

"The larger companies have more at stake if they suffer a loss, so preparation matters more," says Rich Servillas, a director at RSM US LLP. "A lot of this is being driven by cyber insurance, as carriers are increasingly requiring more as a condition of coverage, and that's pushing testing discipline across the middle market."

Frequency of organizational test of incident response plans*



Source: RSM US Middle Market Business Index, Q1 2026

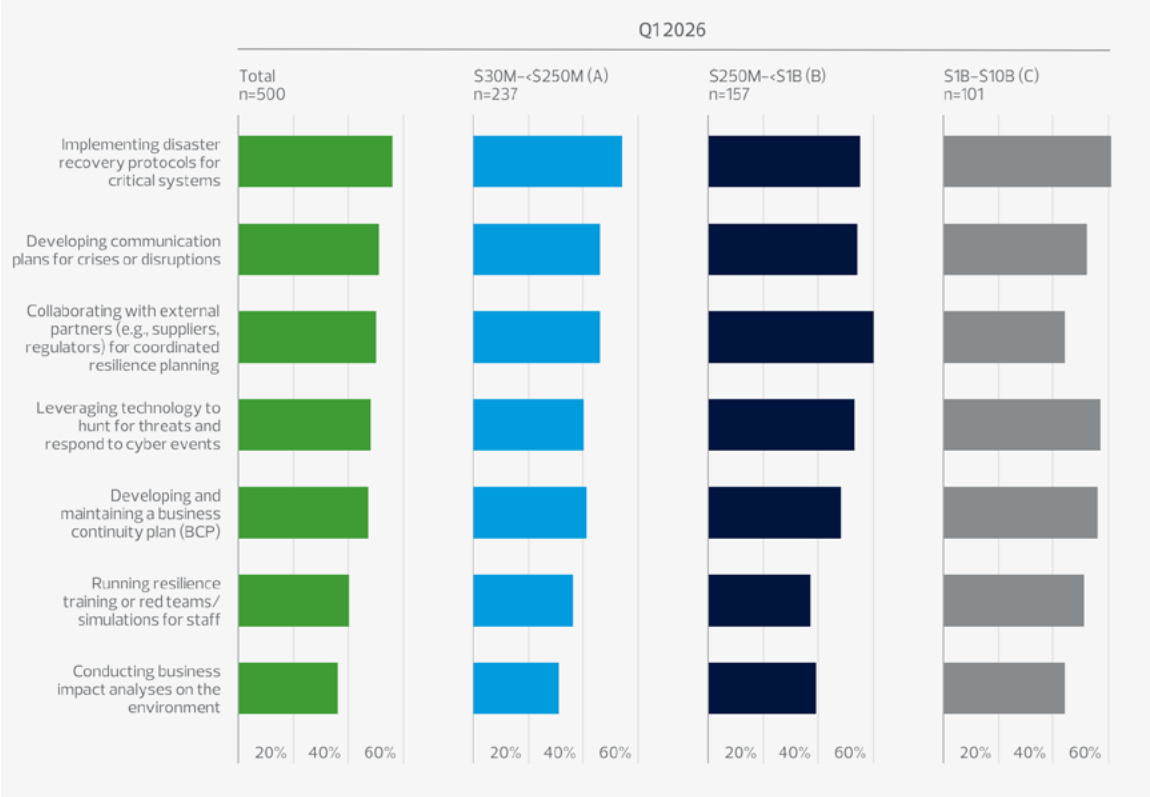
* Base = total sample

AI technology is also now playing a critical role in incident response, making teams more proactive and anticipatory through faster detection, earlier warning of likely attack paths and automated containment of routine threats. It allows detection and response teams to move from a defensive position to more of an offensive mentality, becoming proactive against risk and giving companies a valuable upper hand on threat actors.

"AI is enhancing incident response capabilities, but also enabling predictions," says RSM US Principal Daniel Gabriel. "In some cases, companies are now better at predicting the likelihood of threats and where they're most likely to happen due to the support of AI."

In addition to implementing and testing an incident response plan, middle market companies can take advantage of several key processes to limit business disruptions when cybersecurity events occur. In this year's MMBI survey, the leading processes respondents reported were implementing disaster recovery plans for critical systems (56%); developing communication plans for crises or disruptions (51%); collaborating with external partners for coordinated resilience planning (50%); and leveraging technology to hunt for threats and respond to cyber events (48%).

Processes in place to address disruption and ensure continuity*



Source: RSM US Middle Market Business Index, Q1 2026

* Base = total sample

The Canadian perspective: Four processes to address disruption and ensure continuity were listed by at least half of Canadian survey participants:

- Implementing disaster recovery protocols for critical systems (60%)
- Developing and maintaining a business continuity plan (57%)
- Running resilience training or red teams/simulations for staff (55%)
- Analyzing the business impact on the environment (50%)

Before a cybercriminal can strike, companies need to have a complete understanding of what information they have, implement effective data hygiene and establish thorough data retention policies. Companies also need to understand where their crown jewels reside—what data is most important to the company, and how is it being safeguarded?

"A good understanding of these elements will save companies a significant amount of time if they become a cybercrime victim," says Servillas. "Knowing what data you have and where it resides is a big part of how to mitigate some of that risk."

"AI is enhancing incident response capabilities, but also enabling predictions. In some cases, companies are now better at predicting the likelihood of threats and where they're most likely to happen due to the support of AI."

Daniel Gabriel, Principal, RSM US LLP

In addition, as a best practice, organizations should consider having retainers or prenegotiated relationships with outside counsel, incident response firms or forensics providers before an incident occurs.

"In our case work, the organizations that recover fastest are the ones with those relationships already in place," says Servillas. "The ones calling around for a digital forensics and incident response firm during an active incident can lose 24 to 48 hours of response time."

Methodology

In 2026, RSM closely evaluated the middle market and redefined the segment to encompass companies with annual revenue between $30 million and $10 billion. Today, approximately 125,000 companies make up the modern middle market, employing 50 million people and generating $16 trillion in revenue. **Note:** Due to this redefinition, comparisons of current MMBI data to all trended data prior to Q1 2026 should be interpreted with caution.

The Q1 2026 RSM US Middle Market Business Index survey data was gleaned from a combination of an online sample and a panel of approximately 400–500 executives (the Middle Market Leadership Council) recruited by The Harris Poll using a sample supplied by Dun & Bradstreet. All individuals were full-time, executive-level decision makers working across a broad range of industries (excluding public service administration): nonfinancial or financial services companies with annual revenues of $30 million to $10 billion or CA$30 million to CA$1 billion; and financial institutions with assets under management of $500 million to $500 billion or CA$250 million to CA$10 billion.

These panel members are invited to participate in four surveys over the course of a year that include special issue-based question sets, as well as quarterly index-only surveys; the Q1 2026 survey was conducted from Jan. 6 to Jan. 30 (Feb. 9–Feb. 20 in Canada). Information was collected by phone and online from 501 U.S. middle market executives, including 80 panel members and a sample of 421 online respondents, and 101 Canadian middle market executives. Data is weighted by industry.

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

+1 800 274 3978
rsmus.com

br/4735742/2026/bdt