Companies must remain diligent as cybersecurity threats evolve

RSM US Middle Market Business Index Special Report: Cybersecurity 2025

April 17, 2025

A comprehensive analysis of emerging cybersecurity threats and risk mitigation strategies

Cybersecurity remains a prime concern for middle market companies, as evolving risks present nonstop threats to sensitive data and operations. Organizations face a daily challenge as cybercriminals continue leveraging traditional strategies like ransomware to launch harmful attacks, while new technology such as artificial intelligence and geopolitical concerns present elevated risks.

While the threat environment continues to become more complex, reported breaches have declined in new RSM research. According to findings in the Q1 2025 RSM US Middle Market Business Index survey, nearly one in five (18%) middle market companies experienced a data breach in the previous year, falling from a record-high 28% in last year's data.

The decline in reported breaches is certainly positive, but this year's results are consistent with data from previous years outside of the spike in 2024. In addition, with methods becoming more sophisticated, some attacks may go undetected, highlighting the importance of continuously strengthening controls.

Key findings

- **18%** of middle market executives reported suffering a data breach in the previous year, down from 28% in last year's RSM research.
- **91%** of respondents are expecting to increase cybersecurity spending in the coming year.
- **26%** of survey respondents experienced at least one ransomware attack or demand in the last year, with larger companies more at risk.

The MMBI survey aggregated the responses of 402 U.S. and 101 Canadian middle market executives across a variety of industries. It was conducted from Jan. 6 to Jan. 27, 2025, on behalf of RSM by The Harris Poll.

Inside the report:

Executive summary: While reported cybersecurity breaches drop, risks continue to evolve

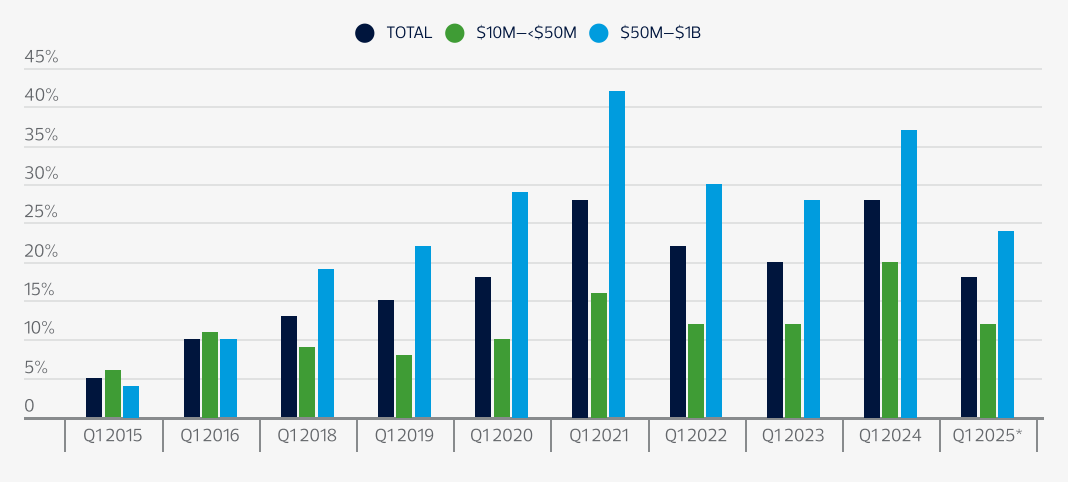
Key takeaways

- **18%** of middle market executives reported suffering a data breach in the last year, down from **28%**.
- Larger middle market companies were twice as likely to suffer a breach.
- Continued vigilance is necessary as cybersecurity threats continue to become more sophisticated.

Middle market companies depend on effective and resilient cybersecurity controls for ongoing sustainability and growth, but the risk environment remains volatile and challenging. Though the percentage of respondents reporting breaches over a one-year term in the Q1 2025 RSM US MMBI survey fell significantly compared to a record high in the previous year, companies cannot afford to be complacent in an environment of constantly emerging threats. As threat actors' tactics, techniques and procedures continually evolve amid advances in generative artificial intelligence and ongoing geopolitical tensions, protective measures must adapt and evolve in tandem.

Nearly 1 in 5 (18%) of the middle market executives surveyed in 2025 said their organizations experienced a data breach in the previous year, a sharp decline from 28% in the 2024 survey and the lowest percentage since the 2020 survey. Drops were seen for both larger and smaller middle market companies, but larger companies were twice as likely to suffer a breach, with 24% of respondents in this segment reporting a breach compared to 12% of their smaller counterparts. However, this discrepancy may be due to smaller companies either lacking sufficient controls to effectively detect incidents or facing less regulatory pressure to report them.

Experienced a data breach in the last year



Source: RSM US Middle Market Business Index, Q1 2025

*TOTAL (n=401); S10M–<S50M (n=176); S50M–$1B (n=216)

The MMBI survey, conducted online and by phone from Jan. 6 to Jan. 27, 2025, on behalf of RSM by The Harris Poll, drew responses from 402 U.S. and 101 Canadian middle market executives across a variety of industries. The data provides insights on smaller ($10 million to less than $50 million in revenue) and larger ($50 million to $1 billion in revenue) middle market organizations in the U.S.—and their responses to many cybersecurity questions revealed large gaps between the two groups. Smaller middle market firms appear to lag their larger counterparts in cybersecurity budgets and staffing, as well as in identity and access management and implementing advanced AI governance protocols.

With reported breaches falling and 91% of respondents reporting an increase in cybersecurity investments, companies generally feel secure in their protective strategies. In fact, 97% of survey respondents are confident in their current security measures, the highest level in the 10-year history of the report. In addition, this year's survey saw a record-high number of companies that carry a cyber insurance policy (82%).

Despite the drop in reported breaches, RSM risk professionals caution middle market companies against getting too comfortable in the face of cybersecurity risks, as the threats are still very real.

Tauseef Ghazi, a principal at RSM US LLP and leader of the firm's cybersecurity practice, believes the reported breaches may have simply normalized after the spike in the previous year's data. "The influx in 2024 is explainable because of the sanctions and the disruption in the financial networks related to the Russia-Ukraine conflict," he says. "After this year's drop in breaches, we are very comparable in terms of historical breach levels in the survey. Therefore, continued vigilance is required, especially with the augmentation of AI to support such malicious activities."

The increased complexity of attacks also may at least partially explain the decline in reported breaches, as some companies may not have identified the presence of an attacker in their systems. For example, when a ransomware attack takes place, the attacker announces themselves to collect the ransom. But now, many bad actors are attempting to access networks and operate silently within them to collect sensitive data.

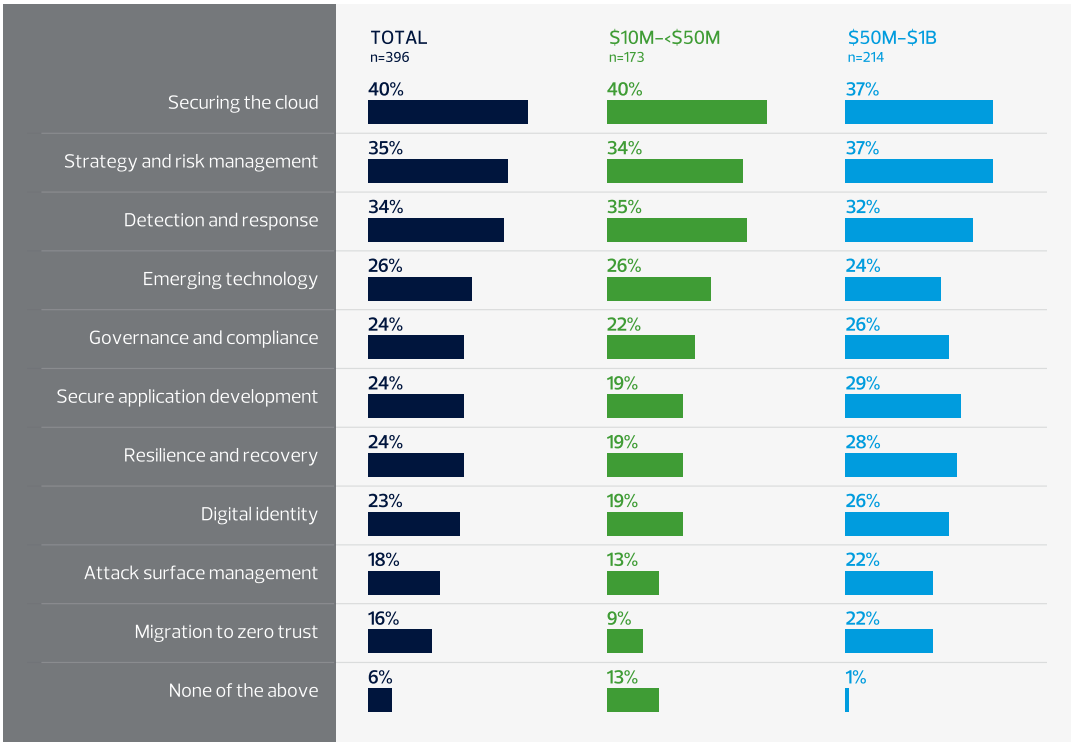
"The scary part for companies is that attacks have become so sophisticated, and they may not be able to detect them," says Daniel Gabriel, an RSM US principal. "If attackers are backing down on ransomware, the goal of the attack is to not disclose yourself."

However, RSM US Principal Matt Franko sees companies taking advantage of some cybersecurity controls and strategies that could also contribute to the drop in reported breaches. "Our No. 1 recommendation still to this day is to develop a strong asset inventory," he says. "We are seeing a lot more organizations start to address asset management and inventory, which is helping them in a variety of other areas, such as vulnerability management and access management. You can do a much better job protecting yourself when you know what you need to protect.

"We have helped a lot of organizations automate their configuration management database with intelligent platforms like ServiceNow," he continues. "Sometimes, it's a combination of tools that creates a consolidated viewpoint of tools and systems. Once that program is up and running, and you're getting a consistent view of your population, you can understand what you have and then go protect it."

Franko also believes that the growing reliance on managed security services and the increased specialization of those platforms have put companies in a stronger position to address evolving threats. "Organizations have invested a lot more in working with companies like RSM and our RSM DefenseTM managed security solution," he says. "Buyers are becoming smarter; they want more sophisticated managed services providers that know and understand their environment."

Top 3 cybersecurity and data privacy initiatives



Source: RSM US Middle Market Business Index, Q1 2025

Meanwhile, Mark Antalik, a managing director at RSM US, highlights the severity of the threat that still exists. "Even with everything that companies are doing to combat cyber risks, a breach is still happening to roughly 1 in 5 organizations," he says. "That's why you need to understand your data and need modern cybersecurity controls in place."

Two significant cybersecurity challenges are projected to persist: staffing and AI governance. Qualified cybersecurity talent has been increasingly difficult to attract and expensive to retain in a very competitive market.

> "After this year's drop in breaches, we are very comparable in terms of historical breach levels in the survey. Therefore, continued vigilance is required, especially with the augmentation of AI to support such malicious activities."
>
> **Tauseef Ghazi**, Principal, RSM US LLP

"Talent is still a huge issue," says Ghazi. "Finding people with the right skill sets is a big challenge, and they are not coming out of universities at that level. Also, we've always cultivated an apprenticeship model in cybersecurity, and people are often not staying long enough to be an apprentice for anyone."

In the past, many companies have relied on offshore talent, but even that staffing strategy is now often out of reach from a financial perspective.

"There are very few people who can solve the complex problems companies have today," says Ghazi. "At a macro level, we are struggling with talent, and offshoring is steadily becoming more and more expensive."

To fill these critical cyber personnel gaps, more companies are turning to increased automation and expanded managed services strategies.

Companies are still generally finding their footing with AI in the middle market, and risks related to data and governance continue to crop up. Organizations need to understand what data they have and manage how it is used with an effective AI governance model.

"AI is not a silver bullet," says Ghazi. "It's still a model that you must train and closely manage. When you're putting data out for AI use, how are you controlling it?"

As attack methods and potential vulnerabilities continue to evolve, protective strategies are advancing in response. To address modern threats moving forward, companies should build proactive cybersecurity strategies by focusing on:

- AI governance
- Data protection and resilience
- Evolving cloud strategies
- Identity and access management
- Automation and engineering
- Managed services

Companies are spending more on cybersecurity, but are those dollars properly directed?

With increased investment, potential security gaps require attention

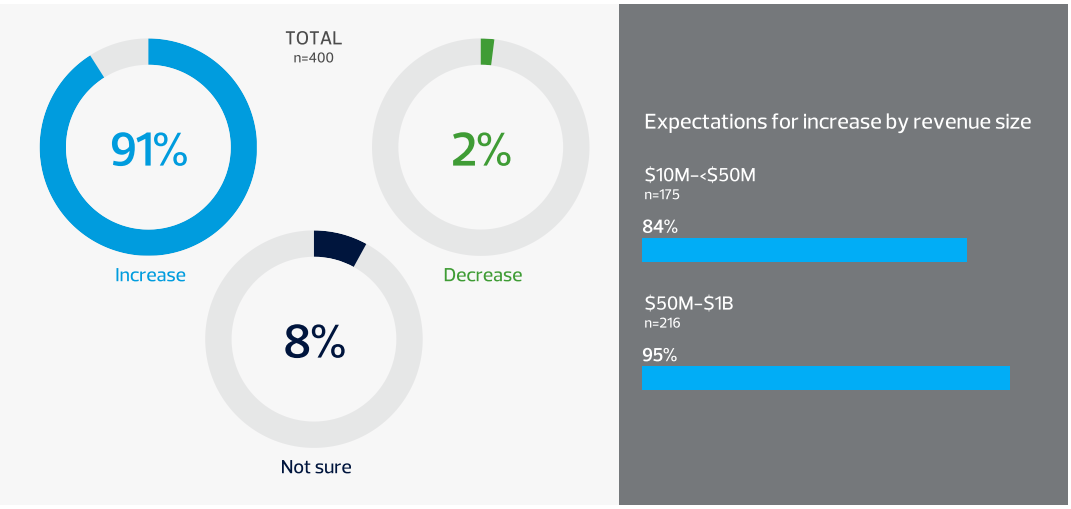
Key takeaways

- **91%** of middle market companies plan to increase cybersecurity spending.
- Cyber budgets in the middle market are most often located under the CEO/president/owner or CFO.
- The IT department is most often responsible for overseeing cybersecurity in the middle market.

With the widespread damage just one cybersecurity breach can cause, middle market companies must continue allocating significant budget and staffing to establishing a sustainable cybersecurity program. While the MMBI data shows that many organizations are indeed increasing their cybersecurity budgets, how they are spending those dollars and building their security and privacy staff could raise concerns.

The data shows that 91% of survey respondents plan on increasing their spending on cybersecurity in the coming year while only 2% project a decrease. However, despite the spending increases, Ghazi sees a common gap in cybersecurity investment strategies.

Expected cybersecurity budget changes in the next year



Source: RSM US Middle Market Business Index, Q1 2025

"Spending is definitely increasing, but that does not always mean it's effective," he says. "Often, companies are paying for more tools, more extensibility and more licensing, but they may overlook key consultative resources that could help drive automation, with better engineering to solve problems at a lower cost and with a lower need for skilled resources to maintain day-to-day tasks."

Survey results showed that for U.S. respondents, the cybersecurity budget is most often located under the chief executive officer/president/owner or the chief financial officer (42% each). While smaller middle market companies follow that pattern (with 45% under the CEO and 35% under the CFO), for larger respondents, the cybersecurity budget most often resides under the chief information security officer (48%) followed by the CFO (47%).

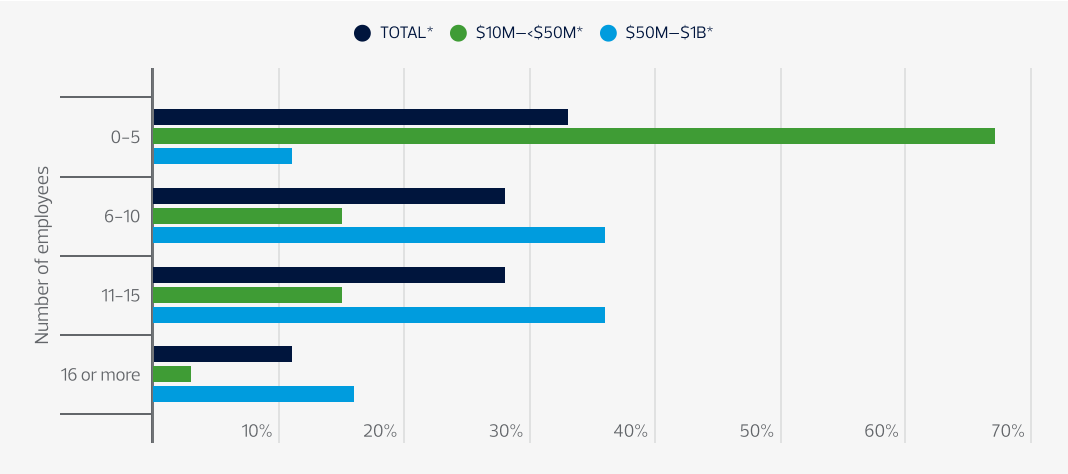
The Canadian perspective: In contrast with the U.S., in Canadian firms the chief technology officer (49%) most often oversees the cybersecurity budget.

The person responsible for guiding cybersecurity planning and execution efforts has a critical role within the organization. When asked who in the organization oversees cybersecurity and related decision making, the top responses in the MMBI survey were the IT department, without a dedicated cybersecurity leadership position (25%); a dedicated CISO or equivalent role (22%); and a chief information officer or equivalent role (20%).

For smaller middle market companies, the IT department has the most responsibility for cybersecurity strategy (26%), followed by the CIO (21%). At larger companies, the CISO leads cybersecurity most often (27%), ranking just ahead of the IT department. For budgeting and planning, more larger companies rely on a CISO compared to smaller organizations, which rarely have a CISO role.

From a staffing perspective, 33% of respondents have five or fewer data security and privacy employees, with 28% reporting they have six to 10 and the same percentage indicating they have 11 to 15. Not surprisingly, larger middle market organizations have a larger number of dedicated internal staff; 36% of those respondents indicated they have six to 10 employees and the same percentage stated they have 11 to 15. Meanwhile, most respondents from smaller middle market companies cited zero to five internal personnel focused on data security and privacy.

Number of employees dedicated to data security and privacy



Source: RSM US Middle Market Business Index, Q1 2025

*TOTAL (n=248); $10M–<$50M (n=95); $50M–$1B (n=152)

The Canadian perspective: On average, Canadian respondents have larger cybersecurity teams, with 39% saying they have 16 or more employees, compared to 11% in the U.S.

As security and privacy grow in complexity, more specialized skill sets will be necessary, and staffing will continue to be a critical focus for middle market organizations.

"Most security and privacy organizations still need help and will need outside help," says Antalik. "Just on the privacy front, the regulatory landscape is so dynamic. There are around 160 countries that have different data protection regulations, and by 2026, 19 U.S. states will have their own data privacy regulations. It's confusing, it's challenging and it's changing all the time."

Confidence in cybersecurity controls is rising, but significant threats persist

Despite optimism, companies cannot afford to lose focus on emerging threats

Key takeaways

- **97%** of middle market executives are confident in current measures to safeguard data.
- **26%** of survey respondents experienced at least one ransomware attack or demand in the last year.
- Defense measures were reported as unsuccessful for **31%** of ransomware attacks.

At this point, middle market companies generally understand the risks cybersecurity threats can pose. But as such threats evolve, companies need to continually address potential vulnerabilities and resist the temptation to get overconfident about current controls.

The share of MMBI survey respondents who are confident in their existing cybersecurity strategies reached an all-time high in this year's data. In fact, 97% of middle market executives reported that they are either very confident or somewhat confident in their current measures to safeguard data, rising slightly from 95% in the 2024 survey and 96% in the two previous years.

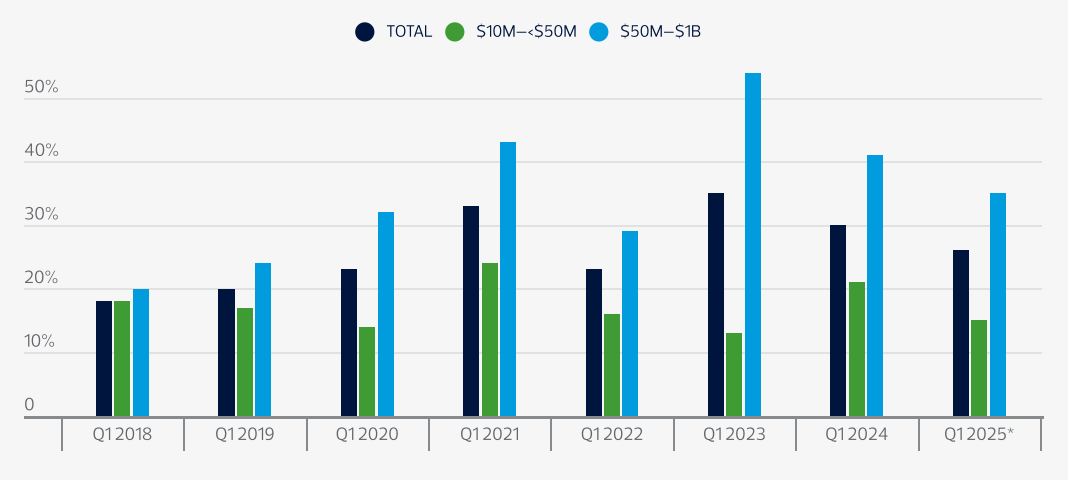
Ghazi suggests that higher spending and more outsourced security have contributed to the high confidence.

"It's likely because they increased investment or, with outsourcing, not many companies are actually facing the cyberattacks themselves," he says. "So that automatically gives you more confidence."

Ransomware continues to be a significant threat to the middle market, with attacks that can restrict access to specific systems, business units or even all company data until certain financial conditions are met. With the interconnected nature of today's businesses and related entities, the harmful effects of these breaches can spread very quickly. In fact, recently ransomware has been in the national spotlight more often after multiple attacks had ripple effects across entire industries and brought productivity to a halt for many companies.

The highly publicized ransomware incidents may be contributing to a continued drop in reported incidents in the MMBI data. This year, 26% of respondents said they experienced at least one ransomware attack or demand in the previous 12 months, a decrease from 30% in the 2024 survey and 35% in 2023. Larger middle market companies are more of a prime target for criminals, as 35% of respondents in this segment reported at least one attack or request, compared to 15% of smaller firms.

Experienced a ransomware attack or demand during the last 12 months



Source: RSM US Middle Market Business Index, Q1 2025

*TOTAL (n=401); S10M–<S50M (n=176); S50M–S1B (n=216)

"I think there were a lot of lessons learned in the last year or two after some of these significant incidents," says Franko. "The major theme comes back to knowing your environment.

"In our maturity and risk assessments, a typical finding is that organizations are not completing a proper business impact analysis or are not completing them across their entire company," he continues. "Organizations often avoid these assessments because they can be resource-intensive [in terms of money and people], but without them, companies often do not have a comprehensive understanding of how many entities they are connected to and the operational and financial damage that could occur if one had an incident. If they do these analyses, they could be more effective in their continuity processes and reduce their risk."

Despite the drop in ransomware attacks, companies cannot afford to lose focus. Just one successful attack can have significant repercussions, from financial losses and regulatory penalties to reputational damage and various opportunity costs, depending on the amount and breadth of downtime and how resources need to shift to manage recovery efforts.

> "I think there were a lot of lessons learned in the last year or two after some of these significant incidents. The major theme comes back to knowing your environment."
>
> **Matt Franko**, Principal, RSM US LLP

Among companies that experienced at least one ransomware attack in the past year, on average, existing security defense measures were reported as unsuccessful for 31% of ransomware attacks, partially successful for 28% of attacks and completely successful for 41% of attacks.

Compared to the previous year, the average percentage of ransomware attacks successfully defended against increased slightly, as did the percentage of unsuccessful defenses, while the average percentage of partially successful defenses decreased by nearly 5%. For the second consecutive year, the survey data showed minimal differences in the effectiveness of ransomware defenses between smaller and larger middle market companies.

As AI plans advance, governance and risk awareness are critical to protect data

AI is transforming business operations, but potential risks must be addressed

Key takeaways

- AI continues to evolve, with governance risks and potential for more complex attacks.
- Monitoring and auditing AI system performance and outcomes is the leading AI governance measure.
- **34%** of smaller middle market companies indicated that AI governance steps are not yet in place.

Artificial intelligence has already revolutionized many key processes for middle market organizations, delivering increased efficiency, insight and productivity. But like other new technology implementations, AI does come with significant risks. Middle market companies must be careful to avoid introducing new vulnerabilities to critical data when integrating AI solutions and expanding their use.

While AI does certainly carry risks, its implementation has rapidly evolved into an imperative for ongoing business success.

"In many ways, AI is still emerging," says Antalik. "Some organizations are further along than others, and some are just at the tip of the iceberg of experimenting with it. But the ones that are scared are missing the boat. While companies that are diving in are bringing on additional risk, if they do things thoughtfully, AI can provide significant benefits across the business."

To successfully deploy AI technology while mitigating potential risk exposure, organizations must implement an effective governance framework. Several frameworks are currently available, including platforms from the National Institute of Standards and Technology (NIST), Google, and Microsoft, as well as guidelines from several countries and industry organizations.

"In many ways, AI is still emerging. Some organizations are further along than others, and some are just at the tip of the iceberg of experimenting with it. But the ones that are scared are missing the boat. While companies that are diving in are bringing on additional risk, if they do things thoughtfully, AI can provide significant benefits across the business."

Mark Antalik, Managing Director, RSM US LLP

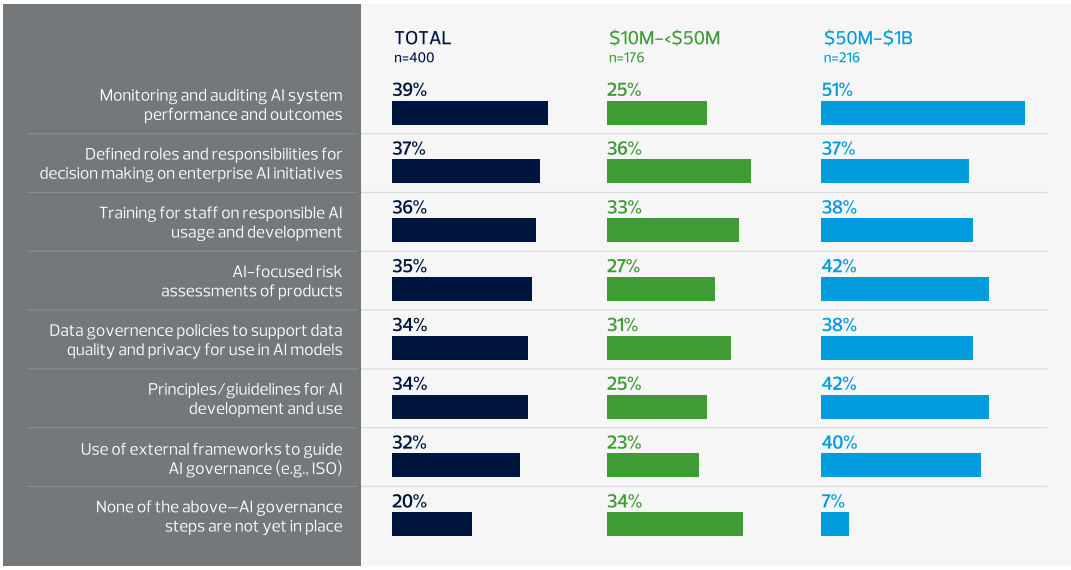
However, data is at the heart of any AI deployment, so data governance—understanding what data assets companies have and where it is stored, processed, transmitted and accessed from—and core AI governance go hand in hand.

"I often talk to clients about how AI governance is really data governance with a few different components added on, and if you struggle with data governance, then you're going to have struggles with AI governance," says Franko. "A vast majority of an AI governance framework is derived from data governance and data protection frameworks. Know your data, protect your data, govern your data. Yes, you must worry about bias and how it makes decisions and whether you are getting the right answers, but you can't get there unless you have those core principles solved."

Regarding leading AI governance practices, MMBI survey respondents identified monitoring and auditing AI system performance and outcomes as the most widely implemented control (39%). Close behind were defined roles and responsibilities for enterprise AI decision making (37%), staff training on responsible AI usage and development (36%), and AI-focused risk assessments of products (35%).

Of note, 34% of smaller middle market companies indicated that AI governance steps are not yet in place. This means that more than a third of these companies are not yet using AI, or if they are, their data is likely at an elevated risk.

AI governance practices



Source: RSM US Middle Market Business Index, Q1 2025

The Canadian perspective: A smaller share of Canadian firms indicate they don't have AI governance in place compared to U.S. respondents (5% versus 20%). This is likely due to Canada's efforts to regulate AI at the federal level.

Beyond AI governance processes, organizations have a growing list of regulatory guidelines to consider when deploying AI strategies. Similar to data security and privacy, AI is not subject to a federal AI regulatory standard in the U.S., but several states are introducing and passing new AI laws. Several specific industries are also rolling out AI standards to promote safe and secure AI usage.

For companies that operate overseas, the European Union has become a pacesetter for AI standards since adopting the first comprehensive set of rules by a major regulator in 2024. Its Artificial Intelligence Act establishes obligations for providers and users depending on the level of risk presented by specific AI tools and applications. Much like the General Data Protection Regulation (GDPR) the EU passed for data privacy in 2018, the AI Act could serve as a global blueprint for AI regulatory actions.

Of course, middle market organizations also must be aware of an entirely new level of threats as criminals harness the power of AI to launch sophisticated attacks. For example, AI is making social engineering attacks feel more realistic by providing attackers with more details about an organization and enabling mimicry of company representatives and leadership with vishing (voice phishing) campaigns and deepfake-enabled impersonations. These attacks are focused squarely on the weakest link in security: people.

"At the end of the day, training your users to understand AI risks is essential," says Franko. "Your people are your first line of defense, and providing them with the right knowledge is critical. At the same time, the technical and procedural controls that support your users must be strengthened, including your organization's capability to monitor and swiftly respond when an incident does ultimately occur."

While companies need to adjust protective strategies and increase awareness to account for more complex AI-supported attacks, the underlying protective strategies are still generally the same as they have always been.

"It's all the same blocking and tackling that has been used for many years," says Franko. "It's making sure you're strengthening your protection mechanisms, monitoring so you can identify when an attack has been successful, getting the bad guys out, learning from it and getting better. AI risks are no different. Your tactics may change, but your principles don't."

Expanding AI risks can understandably be very scary for middle market organizations, but Franko highlights a bright spot.

"The good guys are also armed with AI because it is built into many tools," he says. "So, your defense capabilities are getting better."

How the middle market is building business continuity and resilience strategies

Implementing strategies to limit disruptions and sustain operations

Key takeaways

- **82%** of middle market respondents carry a cyber insurance policy, the most in report history.
- **69%** indicated they are familiar with their cyber insurance policy coverages.
- Communication plans for crises or disruptions is the leading process to ensure continuity.

A company's most valuable asset is its data, and that asset must be secured against persistent cybersecurity threats. In a difficult risk environment, companies have multiple options to protect their data and establish effective business continuity processes. However, companies need to carefully determine the right mix of solutions to align with business processes and successfully protect their environment.

Cyber insurance is one of the most utilized tools to protect data and quickly recover if a cyberattack occurs. However, policies have undergone significant changes in recent years. Rising costs have required adjustments from insurers, with increased premiums in some cases and confirmation of certain conditions and controls before issuance of policies. Despite these changes, though, companies still understand the importance of cyber insurance and the peace of mind it can provide.

Once again, the use of cyber insurance is trending up in the middle market, according to MMBI data. In fact, 82% of survey respondents indicated that they carry a cyber insurance policy, up from 76% the previous year and marking the highest percentage in the history of the report.

"It has gotten harder to get the same coverage levels, and you definitely cannot get them for the same price as you used to," says Alden Hutchison, a principal at RSM US. "There are a lot more requirements, and they make the client prove a lot more security controls are in place to get coverage. But companies are purchasing the policies because they care, and they see the risk."

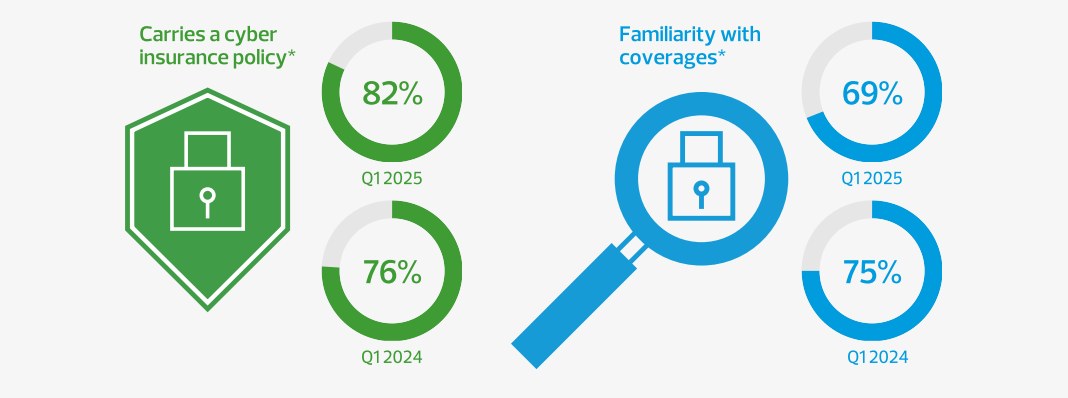
The Canadian perspective: Canadian firms are less likely to have cyber insurance coverage than U.S. companies (68% versus 82%).

Both smaller and larger middle market firms increased their use of cyber insurance in the past year, with smaller middle market companies reporting a rise to 75% from 72% the previous year and larger counterparts jumping to 88% from 83%.

"I'm encouraged," says Antalik. "There have been a lot of changes in the industry, but organizations are moving in the right direction, and cyber insurance is moving from a 'nice to have' to a 'need to have' thing. It just goes to show the state of cyberthreats—it's harder to deal with new threats, so companies need to protect themselves from an insurance standpoint."

Despite the increase in cyber insurance usage, though, fewer companies understand what their cyber insurance policies cover. In the MMBI survey, 69% of respondents indicated they are familiar with their policy coverages, down from 75% in last year's data. Familiarity with policy coverages dropped significantly among smaller middle market respondents (from 66% to 51%) while larger middle market companies reported a drop from 86% to 82%.

Companies that carry cyber insurance and familiarity with coverages



Source: RSM US Middle Market Business Index, Q1 2025

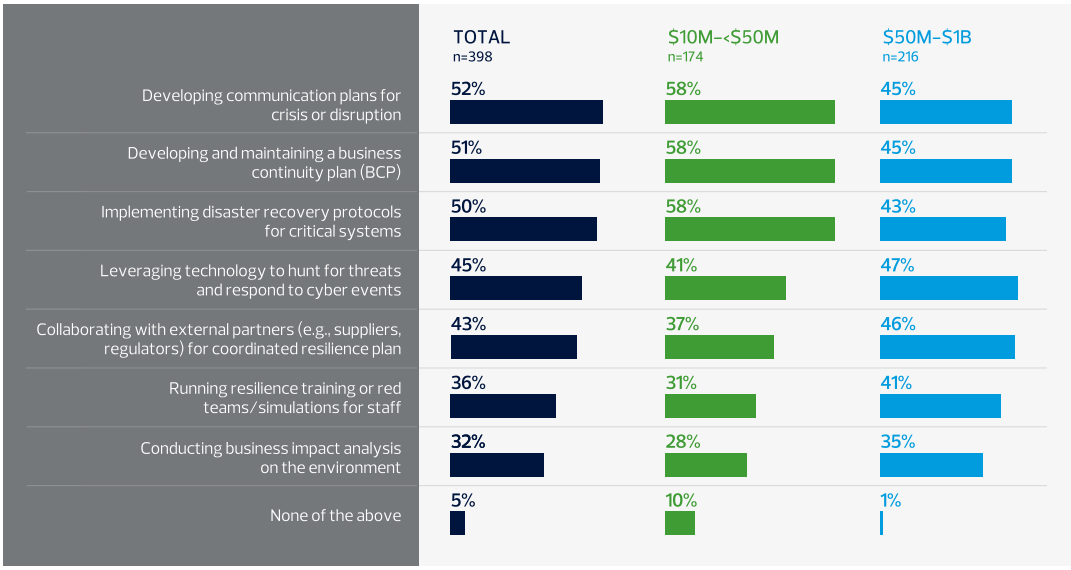
*Carries a cyber insurance policy: Q1 2024 (n=403), Q1 2025 (n=401); Familiarity with coverages: Q1 2024 (n=308), Q1 2025 (n=328)

With the changes to cyber insurance coverage in recent years, Antalik believes that in many cases the parties directly involved with negotiations may be the only people who truly understand policy details.

"With a lot of new policies being established, only those that negotiated them know them in depth," he says. "That's a little scary; what kinds of things are organizations agreeing to and how protected are they?"

In addition to carrying cyber insurance, middle market companies can implement several strategies to limit business disruptions. In this year's MMBI survey, the leading processes respondents reported having in place to address disruption and ensure continuity are developing communication plans for crises or disruptions (52%), developing and maintaining a business continuity plan (51%), and implementing disaster recovery plans for critical systems (50%).

Processes in place to address disruption and ensure continuity



Source: RSM US Middle Market Business Index, Q1 2025

Interestingly, those strategies were also the top three among smaller middle market companies, with each strategy cited by 58% of respondents. Responses from larger middle market companies differed slightly, with leveraging technology to hunt for threats and respond to cyber events ranking as the top continuity strategy (47%), likely driven by more funding availability.

However, in the MMBI survey, only 46% of larger middle market companies and 37% of their smaller counterparts reported collaborating with external partners (e.g. suppliers or regulators) for coordinated resilience planning. These figures represent a potential gap and an improvement opportunity for all middle market companies.

Many businesses are deeply interconnected with external parties and third-party service providers, and recent incidents have clearly demonstrated the potential risks when security controls and business practices fall out of alignment.

"Given how dependent organizations have become on one another, stronger collaboration is essential" says Rich Servillas, a director at RSM US. "To address skills gaps effectively, companies would benefit from being more aligned with the partners and third-party providers that support them."

Hutchison also emphasizes the potential risks involved with not being effectively connected with third-party vendors.

"We have seen so many of these large third-party incidents occur that have disrupted entire industries," he says. "The automotive industry and the health care industry were both hit really hard, and they weren't prepared for how they were going to work with their suppliers to recover from it."

A plan to protect data and recover from a potential cybersecurity incident is not one-size-fits-all. Middle market companies need to have a customized plan in place and adjust it as necessary to align with evolving risks and business processes.

"If you don't have a business continuity and crisis plan of some sort in place, you're at risk of not recovering from a breach quickly enough," says Hutchison. "That plan can keep you from losing your customers, losing the trust of your partners and even potentially losing the business."

Taking advantage of the cloud to strengthen cybersecurity efforts

Ongoing strategic planning is necessary to optimize cloud investments

Key takeaways

- The largest share of midsize companies reported having **21%–50%** of their environment in the cloud.
- Companies cited cloud-native tools and practices as the top cloud tech to enhance cybersecurity.
- Companies need to weigh their options when operating or considering multicloud environments.

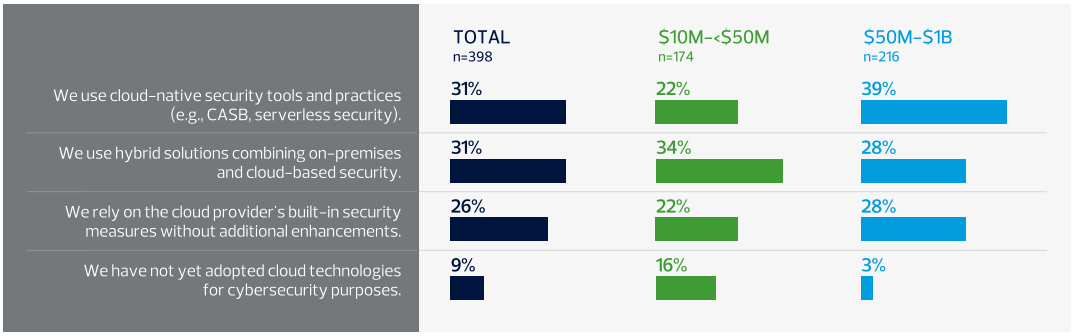
At this point, almost every middle market company has transitioned at least some of its critical data and applications to the cloud for enhanced security. While companies still retain the responsibility for their data security, cloud vendors typically have more extensive security capabilities due to their economies of scale.

MMBI data shows how middle market companies have established different balances of what should reside in the cloud versus on-premises. The greatest share of survey respondents (34%) reported having 21%–50% of their environment operating in the cloud; the next largest group (22%) reported having 51%–75% of their operations in the cloud. For larger middle market companies, the top result (42%) was 21%–50%, while the leading responses for smaller middle market respondents were 21%–50% and 51%–75%, cited by 24% of respondents respectively.

"Migration to the cloud is an ever-evolving journey," says Steve Kane, a managing director at RSM US. "Given the remote workforce and the ability to do anything anywhere, moving things to the cloud to make them accessible and more secure is going to continue to drive adoption."

While moving to the cloud is not a new idea, companies can utilize several strategies to protect their assets there. In the MMBI data, middle market respondents cited cloud-native tools and practices (31%), hybrid solutions combining on-premises and cloud security (31%), and a cloud provider's built-in security measures without additional enhancements (26%) as the leading cloud technologies used to enhance cybersecurity efforts.

Cloud technologies used to enhance cybersecurity



Source: RSM US Middle Market Business Index, Q1 2025

Many middle market companies are being increasingly exposed to multicloud environments, where assets are divided among multiple cloud providers. For larger companies with complex operations and extensive assets, a multicloud environment can help offset the concentration risk that might come with using only one cloud provider. But the strategy almost always brings more complexity than middle market companies truly need.

"The need for a multicloud environment really has to be compelling," says Justin Devine, a director at RSM US. "Concentration risk is worth considering, but the effort, cost and complexity of going multicloud to avoid it are generally not worth the benefit. Unless you are running exceptionally critical workloads where downtime could affect the global economy or endanger people's lives, going multicloud is generally not the best approach. Given today's modern cloud services, it's possible to build extremely resilient architectures without going multicloud. I'd advise consulting with cloud resilience professionals before adding a cloud service provider as the 'easy button'—as building, securing and managing a multicloud environment is anything but easy."

But Devine believes that many middle market companies that choose to implement a multicloud environment may be getting ahead of themselves and introducing unnecessary risk to the organization.

"My honest opinion is that people go multicloud way too early," he says. "I have seen organizations go multicloud when they really don't have a handle on one cloud yet. They double the complexity, split resources in half, make upskilling people twice as difficult, double the attack surface and double the risk."

> "Given today's modern cloud services, it's possible to build extremely resilient architectures without going multicloud. I'd advise consulting with cloud resilience professionals before adding a cloud service provider as the 'easy button'—as building, securing and managing a multicloud environment is anything but easy."
>
> **Justin Devine**, Director, RSM US LLP

However, Gabriel believes most middle market companies that have a multicloud environment got there not necessarily by choice, but because of a transaction. "Most of our clients, you will only see them in a multicloud situation after they acquired another organization," he says. "You end up acquiring someone that is an Azure shop, but you just happen to be an Amazon Web Services shop. The question becomes: What do you do, and is this something you want to manage?"

In most cases, the answer is no. To effectively manage both environments and the complexity between them, companies need duplicative resources with different skill sets. In addition, the authentication source would likely need to be externalized, adding another layer of complexity just to ensure that if something is compromised, the issue doesn't spread to both environments.

"You basically have three options," says Devine. "The first is to double your cloud engineering team so you can support multiple cloud platforms. The second is to refactor and migrate all the workloads to a single platform, and that probably is not worth the effort. Then the third is to limit the risk by transferring the management of the new cloud platform and transferring the risk to a managed service provider. Out of the three options, the first two are not very good."

Ultimately, outsourcing the management of the new cloud environment—the platform with which internal staff lack experience—is the most effective path forward in many situations.

"You have to weigh your options," says Gabriel. "You have two things you must deal with, but your core capabilities likely only align with one of them. Can you find a qualified advisor to help you? They can support you as you grow as an organization and determine where your cloud journey is eventually headed."

Developing a comprehensive digital identity approach

As the security perimeter shifts, digital identity strategies must evolve

Key takeaways

- Companies need to understand, clearly define and control how much access users truly require.
- Respondents cited centralized IAM systems with MFA support as the top digital identity strategy.
- Effective digital identity processes can boost efficiency while supporting increased security.

As security threats continue to evolve, the network no longer represents a company's security perimeter. In today's cybersecurity environment, identity is the new perimeter. With internal users, applications, customers and services providers needing varying levels of access to systems while hackers are constantly attempting to break in, middle market companies need to understand, clearly define and control how much access, if any, employees and vendors need to perform specific tasks.

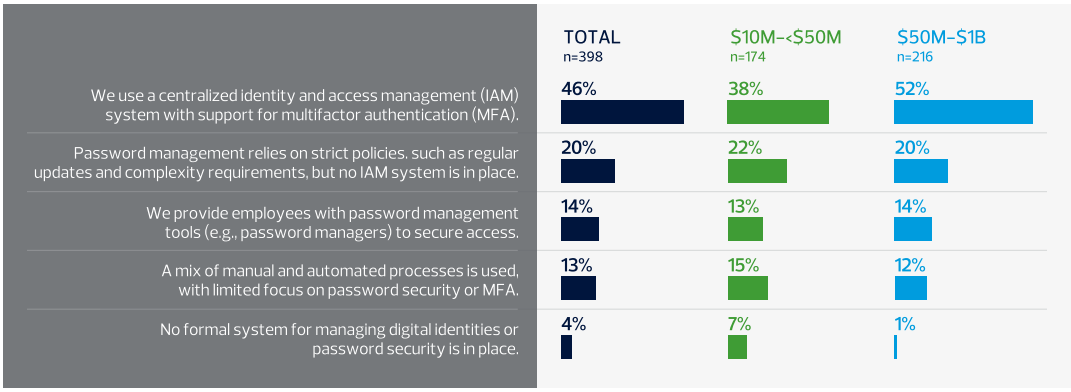
"A truly effective digital identity strategy must cover capabilities and services to address inherent and compliance risk, introduce operational efficiencies, and be flexible as access requirements for humans and nonhuman resources dynamically change," says Omer Arshed, a partner at RSM Canada. "As organizations go through digital transformations and continue to invest in technology, the right approach can protect sensitive data and improve the digital experience for both customers and employees."

> "Many organizations see digital identity as a large initiative that can introduce complex change and affect the organization. On the contrary, digital identity investments, planned and implemented in the correct manner, are enablers and improve the digital experience for employees and customers while reducing inherent risks and creating cost efficiencies."
>
> **Omer Arshed**, Partner, RSM Canada

In this year's MMBI survey, the top method middle market respondents said they are leveraging to manage digital identity and secure systems access is a centralized identity and access management (IAM) system with support for multifactor authentication (MFA). As identity is a multifaceted service addressing employees, customers and applications, organizations must prioritize quantifiable risk reduction and enable foundational controls such as MFA. IAM with support for MFA was cited by 46% of overall survey respondents and was the leading method for both large (52%) and smaller (38%) middle market organizations.

The second-leading digital identity method (20%) in the MMBI survey was password management that relies on strict policies, such as regular updates and complexity requirements, but with no IAM system in place. Providing employees with password management tools to secure access ranked third at 14%.

Methods used to manage digital identities and secure systems access



Source: RSM US Middle Market Business Index, Q1 2025

"Some people just think of identity as a username and password that provides access to different groups and functions," says Kane. "But people don't often consider that sometimes even the lowest permissioned user can be an internal threat if their credentials are spoofed or obtained through social engineering or other methods. With a credential, a threat actor has the keys to the kingdom and can start getting access to data."

Effective digital identity processes have rapidly evolved into a critical element of a middle market cybersecurity strategy. Unfortunately, some companies may see digital identity as an obstacle to productivity when the opposite is true: It can boost efficiency while supporting increased security.

"Many organizations see digital identity as a large initiative that can introduce complex change and affect the organization," says Arshed. "On the contrary, digital identity investments, planned and implemented in the correct manner, are enablers and improve the digital experience for employees and customers while reducing inherent risks and creating cost efficiencies."

Leveraging managed services to address talent gaps and mitigate cyber risks

Cybersecurity and talent challenges emphasize increased need for outsourcing

Key takeaways

- The need for outsourced cybersecurity solutions is greater than ever.
- Cybersecurity risk and compliance management is the leading outsourced cybersecurity function.
- External providers can offer valuable experience and perspective on emerging issues.

Outsourcing is a proven strategy for success within many middle market businesses, filling talent gaps with trusted third-party personnel. The need for outsourcing is even more pronounced within the cybersecurity function, where a challenging talent environment has made it difficult for middle market companies to attract and retain security staff with the necessary knowledge and experience.

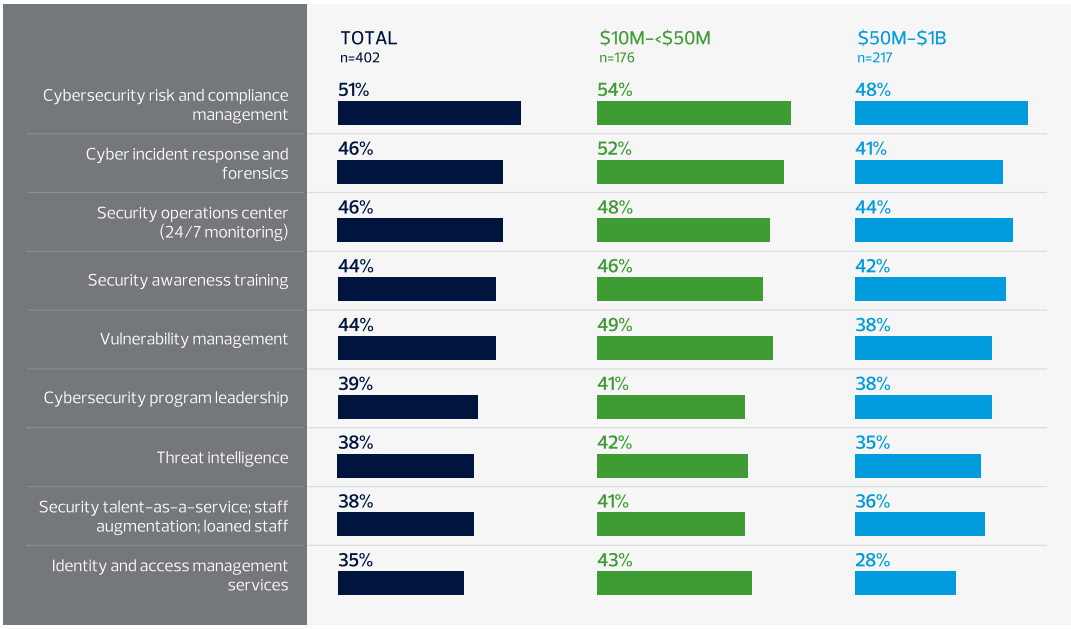
"The need for outsourcing is probably greater than it's ever been," says Kane. "As organizations focus on doing more with less, the cyberthreats are still extremely prevalent and they are not going anywhere."

"Although I think that the talent shortage is starting to shrink a bit as AI creeps in and starts to automate more functions," he continues, "it's still going to take at least 10 years to get to a point where we are not in a talent shortage mindset."

For now, many middle market companies typically cultivate an ecosystem of outside vendors that can address talent gaps while increasing productivity, efficiency and security. But in an optimal scenario, companies can obtain all outsourced services with a single trusted vendor. With vendor consolidation, services are more consistent, and communication is more efficient with several services under one roof and a single point of contact.

In the MMBI data, the leading cybersecurity function outsourced by respondents is cybersecurity risk and compliance management (51%). Other leading outsourced functions include cyber incident response and forensics (46%), security operations center (24/7/365 monitoring) (46%), security awareness training (44%), and vulnerability management (44%).

Cybersecurity functions currently outsourced



Source: RSM US Middle Market Business Index, Q1 2025

"It's hard for middle market companies to keep the necessary talent internally, so they often don't have a choice but to go outside," says Antalik.

In addition to providing more experienced personnel, outsourcing gives companies direct access to advanced technology that would be out of reach otherwise. "A lot of organizations don't have the financial backing to buy all of the requisite tools and instruments necessary to address today's complex threats, on top of managing and maintaining the right staffing levels," says Kane.

In most cases, the most significant benefit related to outsourcing is the perspective from a qualified external provider that understands emerging issues and can leverage experience gained with other clients.

> "The need for outsourcing is probably greater than it's ever been. As organizations focus on doing more with less, the cyberthreats are still extremely prevalent and they are not going anywhere."
>
> **Steve Kane**, Managing Director, RSM US LLP

"Many organizations hire managed services providers like RSM to come in as an independent lens to look at their programs and help them identify actual gaps and make recommendations to make security programs better," says Antalik. "With internal personnel, human nature can get involved, and people may not want to lift up the rug and look under it.

"Firms like RSM work with hundreds and hundreds of different clients," he continues. "We see a lot of different things and bring those industry and client leading practices to create effective security solutions. It's no fault of internal personnel; they just don't have the perspective of what other organizations are doing and what's working against current threats."

The cybersecurity environment is only becoming more challenging, making managed security services a more attractive option for middle market companies. With an effective outsourcing approach, companies can gain direct access to the talent and tools necessary to address evolving and persistent cybersecurity threats.

Methodology

The Q1 2025 RSM US Middle Market Business Index survey data was gleaned from a panel of approximately 1,600 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 $10 million to $1 billion or CA$10 to CA$1 billion; and financial institutions with assets under management of $250 million to $10 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 2025 survey was conducted from Jan. 6 to Jan. 27. Information was collected by phone and online from 402 U.S. middle market executives, including 164 panel members and a sample of 238 online respondents, and 101 Canadian middle market executives. Data is weighted by industry.

+1 800 274 3978
rsmus.com