



2023 RSM US MMBI Cybersecurity Special Report

TABLE OF CONTENTS

Executive summary.....	2
As the business environment evolves, the middle market sharpens its focus on cybersecurity.....	4
Information and data security	6
Cyber insurance.....	8
Ransomware attacks	10
Business takeover threats.....	12
Privacy protections compliance.....	14
Migration to the cloud to ensure data security.....	16
Methodology.....	17
Biden team makes cybersecurity a priority for government—U.S. Chamber of Commerce commentary	18
The shift toward managed security services in the middle market.....	19

Executive summary

Breaches fall slightly, but the threat environment remains elevated

The middle market remains a primary target for cybersecurity attacks as the threat environment has evolved over time. In the past year, companies have dealt with a wide range of threats, including ongoing geopolitical risks, an uncertain economy and the lingering effects of the COVID-19 pandemic. Now, more than ever, threats can come from several directions, so companies need to prepare.

As the amount and scope of cybersecurity attacks have increased in recent years, even the breaches at larger organizations that previously made national headlines barely garner public attention. We know that no company is completely immune to a breach, and attackers will work to find the most vulnerable targets for an attack. That often means focusing on smaller and midsize companies that may not have the budget and internal resources of larger organizations.

The positive news is that despite the increasing pressure from various threats, the number of reported breaches is slightly down as organizations generally appear to take cybersecurity challenges more seriously. But despite easing, the number is still elevated, and companies cannot afford to relax. Instead, they must continue to focus on expanding protections and implementing cybersecurity strategies that align with company investments and goals while criminals relentlessly pursue vulnerable systems, data and intellectual property.

"A critical element of any cybersecurity strategy is for boards to authorize investments in organizational, educational and cultural changes needed to close the cybersecurity governance gap and to develop a contextual understanding of how a company's business systems function and interact. There are no 'check-the-box' solutions for cybersecurity governance," says Rod Hackman, RSM cybersecurity risk and board advisor.

Middle market leaders provided a valuable look into their ongoing cybersecurity efforts in a 2023 RSM US Middle Market Business Index first quarter survey. The survey polled 406 senior executives at midsize organizations about their cybersecurity and data privacy challenges, revealing the frequency and severity of attacks and providing details about ongoing threats. The survey research offers a glimpse into how the largest segment of the U.S. economy is implementing controls and strategies to address security threats and combat the tactics of cybercriminals. In almost all cases, research provides specific data for smaller (\$10 million to less than \$50 million in revenue) and larger (\$50 million to \$1 billion in revenue) middle market organizations.

According to the MMBI data, 20% of middle market executives claimed their company experienced a data breach within the last year, representing a slight decline from 22% in last year's survey. Larger middle market organizations were once again more at risk (28%) compared to their smaller counterparts (12%). Still, they showed a small reduction in attacks while those at smaller companies stayed the same.

Consistent with the decline in reported attacks, the number of executives anticipating unauthorized users attempting to access data or systems in 2023 eased to 68% from 72% last year. However, that is still a large number, and companies appear to recognize the need to invest in more cybersecurity resources. This investment is demonstrated in the MMBI survey data, as 77% of respondents disclosed that they have a dedicated function focused on data security and privacy, a considerable jump from 60% last year.

In addition, the majority of middle market executives understand the importance of carrying a cyber insurance policy. The RSM survey found that 68% of companies have such a policy, up from 61% last year. The data shows that the number of smaller companies that utilize cyber insurance rose slightly while larger companies with policies rose significantly to 70% from 57% in 2022.

Data privacy will likely soon become a priority of many middle market risk strategies, with state-level laws going into effect in California, Colorado, Connecticut, Iowa, Utah and Virginia and the scope of many others coming into focus. The basis of these laws is to specify who should collect and possess sensitive data and how to store it. Simply put, companies no longer need to just detail how information from customers and users is stored, but why they need that data in the first place. The inspiration for these U.S. laws is the European Union's General Data Protection Regulation, a landmark piece of legislation that took effect in 2018 and served as a blueprint for other data privacy standards worldwide.

The MMBI research shows that data privacy is on the radar of most middle market companies, with 57% of executives disclosing they are familiar with the requirements of the GDPR, a slight decline from 2022. However, 96% of respondents report that preparing for emerging privacy legislation or regulations is at least a priority of minor importance, the same amount found in last year's survey.

The cybersecurity environment is expected to remain volatile for middle market companies, with current threats projected to continue and new threats periodically emerging at the hands of skilled criminals. Benchmarking opportunities and perspectives from peers are critical tools to fight back against threats and develop effective cybersecurity strategies. To that end, RSM has developed this report to provide relevant middle market cybersecurity insights and data privacy trends, as well as to outline tactics organizations can utilize to strengthen security and privacy programs.

'A new learning experience'

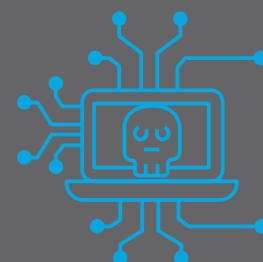
"It won't stop anytime soon, and it's getting more expensive to try to mitigate these risks. It's an everyday challenge for everybody. About the time you think that you're getting ahead, something new comes out. So, every day is a new learning experience."

Chief Financial Officer, utilities company

Are you confident in your cybersecurity program?

Every organization is facing an elevated level of cybersecurity risks, with threats evolving on a frequent basis. If you don't know where you stand, our cybersecurity Rapid Assessment® can provide the insight and detail that you need.

[Identify your risks](#)



As the business environment evolves, the middle market sharpens its focus on cybersecurity

Companies take a more proactive security stance, but challenges lie ahead

While geopolitical conflicts and the uncertain economy have created significant challenges in the middle market, the COVID-19 pandemic resulted in a seismic shift in the entire business environment, with aftereffects still being felt today. But with those dramatic changes, middle market companies have also made strategic process changes that show how seriously they are taking cybersecurity.

Changes during the pandemic are still felt today

When the pandemic initially struck, many companies rapidly transitioned to a remote work strategy, upending the traditional office environment and requiring new technology investments ranging from productivity software to more extensive cloud storage.

"Even organizations that could never fathom the idea of having remote servers and cloud systems had to make it work because their workforce was all remote," said Tauseef Ghazi, RSM principal and national leader of security and privacy services. "The biggest amount of digital transformation that you could have imagined in the middle market has taken place because of COVID-19."

Driven by the pandemic, organizations have relied more heavily on technology over the last three years. And with this transition, they have been forced to become more tech savvy. In 2020, year one of the pandemic, middle market companies were scrambling to find and implement solutions. In year two, companies were working through their new environments and making adjustments where necessary. Now, in year three, everything is up and running, and it's a new way of running the business.

"Over the last three years, organizations have become more digital—the market has forced them to," commented Ghazi. "Regardless of whether it is a manufacturing, hospitality or automotive company, they are all becoming digital companies. In a lot of ways, they all now resemble tech firms."

Cybersecurity investments are following in the footsteps of tech advances

With the increasing digital shift, companies moved more infrastructure out to the internet and the cloud; at first, more compromises initially took place because it was low-hanging fruit for criminals. However, as **digital strategies** have evolved, cybersecurity strategies have also advanced.

For example, the MMBI survey found a sharp increase in the number of middle market companies with a dedicated function focused on security and privacy, as well as significant increases in the number of people responsible for data security and privacy reporting directly to the CEO. These transformational adjustments show that middle market companies understand the importance of cybersecurity as an ongoing effort, not just as challenges arise.

Ghazi describes the correlation between increased digital investments and strategic changes. "Now that you've made these digital investments and put your crown jewels on display, you want to make sure you're also making the necessary investments to protect them."

Staffing and structural challenges ahead?

However, middle market companies will need to keep an eye on the evolving talent environment. With a growing emphasis on more digital investments across the business world, keeping up with necessary staffing has led to the need for increased investment. The demand for experienced IT resources to manage and protect proprietary information has created a more dynamic IT workforce and has pushed costs up.

In a difficult labor market with unemployment hovering around 3.5% and with a cybersecurity presence now a critical element of doing business, middle market companies generally have two choices for structuring their cyber functions: They can develop in-house talent and procure the tools and technology necessary to support it, or they can leverage a vendor or outside advisor for a **managed security services** approach. In some cases, a hybrid strategy, with elements of both tactics, may also be appropriate.

In addition, as middle market companies continue to develop digitally, the tasks necessary from a cybersecurity resource perspective will become more complex. For example, companies are starting to utilize hybrid cloud environments that require more attention; and identity and access management will become more critical as users need different levels of access to the growing numbers of solutions and platforms necessary to support the IT environment.

This growing complexity should **compel boards** to become more involved in understanding the digital systems they govern and invest more time with management to convert complex jargon into the language of business.

The cybersecurity environment will continue to be more challenging as the business world becomes more digital and talent becomes more costly. But as the last three years have shown, the segment is willing to adapt and make investments where necessary.

‘You just keep trying’

“I have implemented multifactor authentication on all of our Outlook and Office products, and we have MFA required on all of our financial accounting software. But they're still prone to attacks because shortly after we implemented MFA, my email got hacked. You just keep trying.”

Controller, construction company

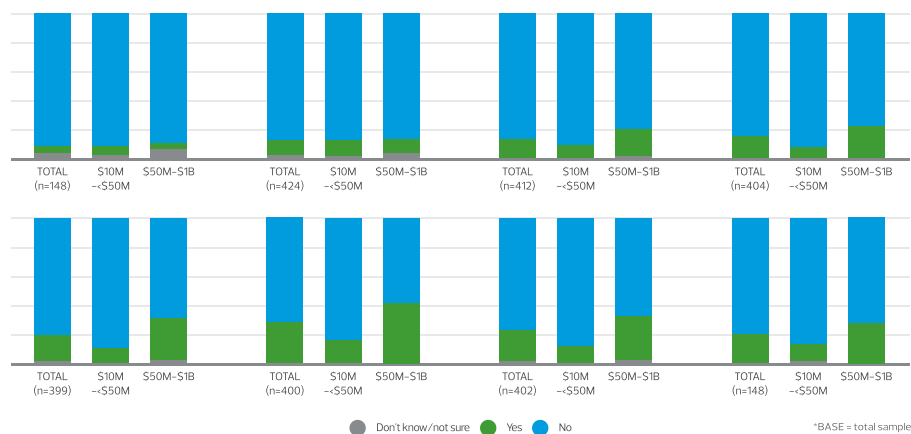
Information and data security

As each year passes, the cybersecurity environment becomes seemingly more complex for middle market organizations. Companies still contend with the effects of the COVID-19 pandemic and managing various **workforce strategies**. At the same time, the Russia-Ukraine war and other global issues create a ripple effect of risks at home. As the year has progressed, an uncertain economy has added further complexity to the business environment.

In addition to creating everyday business challenges, these issues have contributed to a landscape where new vulnerabilities can emerge as companies shift resources to keep the business healthy. And while criminals have always been opportunistic, they are consistently changing attack methods and taking advantage of technology to make more of an impact, concurrent with technology improvement taking place at more legitimate businesses.

"Many activities have gotten pretty sophisticated, and there is not always a human behind attacks," said Ghazi. "Many programs now are automated and running constantly in search of security gaps to exploit."

The RSM MMBI survey shows that breach risks remain elevated, but the number of reported breaches has fallen slightly for the second straight year as **protective strategies** continue to evolve. This year, 20% of middle market executives reported experiencing a data breach in the last 12 months, compared to 22% in last year's survey. Despite the slight decline in reported breaches, the amount is still twice as high as it was just seven years ago.



The number of executives at smaller middle market companies that reported a breach remained consistent with last year's data (12%), while larger organizations reported a decline in breaches (30% in 2022 to 28% this year).

Consistent with fewer reported breaches, the number of middle market executives who expect a breach attempt in the coming year also fell slightly. In this year's survey, 68% of participants indicated that unauthorized users are somewhat likely or very likely to access data or systems, down from 72% last year but still up from 64% in 2021 and 55% in 2020.

68%

of executives believe unauthorized users will attempt to access their data or systems in 2023.

Once again, confidence in cybersecurity strategies is very high in the middle market. For the second straight year, 96% of respondents were confident in their current measures to safeguard data, matching last year's record high.

Ghazi attributes some of the high confidence to the increase in cloud adoption. "Companies have gotten more confident as they have started moving to the cloud," he said. "But that can create a false sense of security, depending on your strategy."

Another reason for increased confidence is an apparent shift in strategy to invest in more cybersecurity resources. The number of executives who reported a dedicated function focused on security and privacy increased significantly to 77% this year, up from 60% in last year's survey.

In addition, many middle market companies appear to have changed their reporting structure in the last year. In this year's survey, 40% of executives report that the person most responsible for data security and privacy reports directly to the CEO, an increase from 25% last year. That number actually fell slightly at smaller middle market companies (38% in 2022 to 33% in 2023), while it rose significantly at larger organizations this year (16% to 43%).

The rise in investments is further emphasized by the number of middle market executives who reported purchasing new or upgraded hardware in response to publicized data security breaches. This past year, 56% of companies said they implemented new hardware, compared to 40% last year. The increase is even more pronounced at larger middle market companies, with 63% making new hardware purchases in contrast to 36% in 2022.

Even as cybersecurity risks continue to expand and evolve, it's clear that middle market companies are making a **concerted effort to address** emerging issues and protect critical information and assets. While the incremental decline in breaches is good news, companies must remain aware of the persistent threat environment around them and adjust strategies, controls and investments to align with risks and overall business objectives.

'Education is critical'

"We're going to continue to invest in software and technology to add layers of protection. We're going to continue to invest in education for our employees. And really and truly, I think the education for our employees is just as important as every layer of defense we can put in our technology."

Chief Financial Officer, utilities company

Cyber insurance

The cyber insurance landscape has undergone many significant changes in recent years, as insurance companies have imposed more restrictions on qualifications and coverages after dealing with more and more expensive breaches. Cyber insurance is still a valuable element of a comprehensive cybersecurity strategy for middle market companies. But as always, companies need to make sure a policy makes sense, with the appropriate coverages for their needs.

A well-defined cyber insurance policy can help organizations recover quickly from a breach. With the high number of events in recent years, if a middle market company has not had to use cyber insurance themselves, they likely know of a peer that has leveraged a policy to help relieve some of the harm in the wake of a breach. However, companies must understand how the insurance landscape has changed and the alterations in the policy limits and the extent of available coverages.

"It's getting harder to get insurance, and policies are getting more expensive," said Matt Franko, RSM principal. "Recently, I have been asked whether or not organizations should have insurance, and of course, the answer is yes."

The RSM MMBI survey found that 68% of respondents currently utilize a cyber insurance policy to protect against internet-based risks, increasing from 61% in last year's report. A closer look at the data shows that the number of smaller middle market companies with cyber insurance increased to 67% from 65% in 2022, while larger companies that reported carrying a policy jumped significantly to 70% this year from 57% in 2022.

68%

of middle market companies carry a cyber insurance policy, up from 61% last year.

Given the current risk landscape, it's not surprising that most middle market companies have seen rising cyber insurance costs. In this year's survey, 70% of respondents reported increased policy premiums, up slightly from the 67% who reported increases in 2022. Consistent with last year, only 2% saw a decrease in premiums.

70%

saw an increase in cyber insurance policy premiums. Only 2% saw a decrease.

"A big change in premiums occurred over the last year," said Franko. "But we are now starting to see the market begin to level out."

Nearly half of middle market executives (49%) reported an increase in covered risks, compared to 52% in last year's report. The increase is much more significant for larger middle market companies, with 62% seeing more extensive coverage, compared to 33% of smaller organizations.

Cyber insurance policies are generally fairly modular, with several coverage options that can be combined to meet a company's specific needs. The most popular coverages reported this year were data destruction (65%), hacking (62%), business interruption (56%) and failure to safeguard data (55%).

However, the RSM MMBI data shows a large drop in coverage for extortion (including ransomware attacks), with 51% of executives carrying coverage compared to 64% in 2022. Similarly, 50% of organizations report coverage for theft, compared to 62% in last year's data.

"Some carriers are simply removing ransomware from available coverage," commented Franko. "Insurance companies were suffering big losses, so some decided that they just were not going to cover it anymore."

With some changes in policy terms and coverages, fewer middle market executives reported being familiar with what their policies cover. Among middle market companies that carry cyber insurance policies, 62% of executives reported they are familiar with their coverage, a decrease from 67% last year. Awareness of coverage for larger middle market companies rose to 84% from 80% last year, while smaller company awareness decreased sharply to 36% from 53%.

"It's critically important to have a holistic picture of what is and is not covered, not just in your cyber liability insurance, but across all of your insurance platforms," said Franko. "There can be some crossover—some things might be covered twice, or things may not be covered in your cyber liability insurance but covered by another policy."

Franko outlined a strategy for leveraging cyber insurance. "You have to understand what your risk is, what your risk thresholds are, what you are willing to pay money to mitigate and what you're willing to accept, and then transfer the rest to an insurer," he said. "A company should not just blindly go out and get insurance. That's a good way to overspend."

'Jumping through necessary hoops'

"We have had cyber insurance for probably eight years, and the hoops we now have to go through ... the first year we didn't (have hoops)—we bought a policy, I think it was \$17,000, and now it's closer to \$40,000, and we have to fill out an extensive questionnaire. It's becoming a lot more selective. The reason we have it is that if there is a cybersecurity breach, they become a partner with us in fixing the problem."

Chief Operating Officer, nonprofit organization

Ransomware attacks

Consistent with previous years, ransomware remains the primary cybersecurity threat to middle market companies, with attacks resulting in several layers of harmful consequences. Ransomware has grown in popularity among threat actors, as it represents a low-risk, high-reward opportunity to generate revenue by taking control of a company's systems or sensitive data.

The threat has escalated in recent years, with ransomware attacks becoming even easier to launch as threat actors have taken advantage of evolving technology. For example, ransomware-as-a-service applications are now available to would-be threat actors lacking technical skills. They rely on the capabilities of the software developer.

Ransomware threats encompass more than just simple breaches. Attackers who find their way into a victim's systems or servers can essentially hold a business hostage, demanding a payout to restore systems to working order. But that is often just the tip of the iceberg, as attackers have become even more relentless, and incidents have become even more complex.

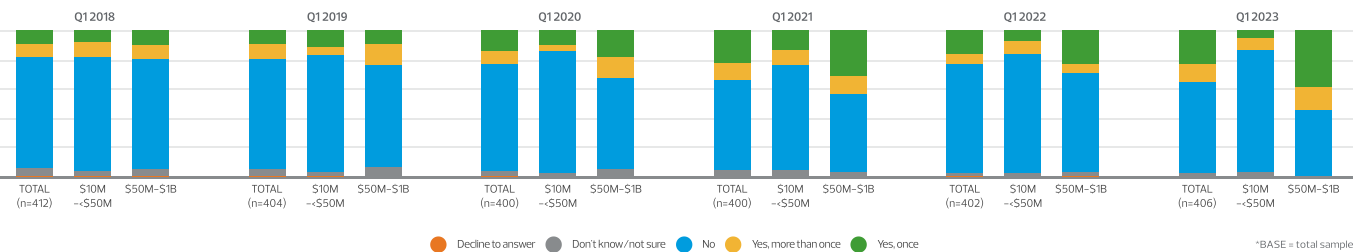
"It's not just the ransom," said Sean Renshaw, RSM senior director. "It's also the reputational risk, especially if the attacker starts calling your customers or clients and telling them that their data was stolen, as we have seen recently."

Renshaw further explained how ransomware attacks can result in significant costs beyond the potential ransom payment. "Over the past few years, there's been a significant increase in business interruption costs. Companies are essentially out of business, unable to ship products or send out invoices to get paid. The cost of recovery has started to trend upward as well."

In the past, many companies relied heavily on cyber insurance to alleviate the effects of ransomware attacks, but some insurance providers have reduced or even eliminated coverage for ransomware.

"We see a lot of companies use their insurance policies as their safety net," said Renshaw. "But I think that is going to become less and less of a safety net as time goes by."

In this year's RSM MMBI data, 35% of middle market executives disclosed that they experienced a ransomware attack or demand, up from 23% last year. Larger middle market companies reported a sizable increase, with 54% indicating an attack or demand this year compared to 29% in last year's report. At the same time, smaller organizations saw a slight decline in incidents to 13% from 16% last year.



The number of respondents in the MMBI research who know a peer whose company suffered a ransomware attack also increased compared to recent years. In this year's survey, 45% reported that they know someone whose firm has been the target of an attack, compared to 41% last year and 42% in 2021.

Middle market executives understand that ransomware will continue to be a significant threat. The number of MMBI survey respondents who believe they are at risk for a ransomware attack in the next 12 months stayed fairly consistent—63% compared to 62% a year ago. Seventy-nine percent of respondents from larger middle market companies feel they are at risk for a potential attack this year, compared to 46% of smaller companies.

63%

of executives feel they are at risk for a ransomware attack in 2023

While the RSM MMBI data showed an increase in reported attacks, many metrics indicate that ransomware attacks actually declined over the past year. For example, a [recent SonicWall report](#) showed a 48% drop in ransomware volume in the United States in 2022.

The decreases shown in other surveys are due to various factors, including sanctions imposed on organizations paying a ransom and enhanced cybersecurity measures implemented by companies. In addition, the Russia-Ukraine war has diverted the traditional threat actors' attention away from ransomware attacks as they wage a cyber battle with each other. In addition, the war has led to increased oversight of financial institutions in Eastern Europe and the freezing of assets, disrupting many networks that previously transmitted ransomware assets.

"Ultimately, that's where most of the money is traditionally moving," said Ghazi. "At some point, the Bitcoin has to be transformed into real cash, and that happens at home."

Renshaw has an explanation for the possible discrepancy between the increase in reported ransomware attacks in RSM's data and reports of decreased incidents elsewhere.

"It's different now," Renshaw explained. "In the past, when big entities were hacked, it was front-page news for days. Now, entire cities are hit with ransomware, and it barely registers as a blip on the news. As a result of the reduced stigma surrounding companies becoming ransomware victims, there has been an increased willingness to report cyber attacks to law enforcement."

The ransomware environment will continue to be complicated and very dangerous. Even if attacks are dropping because of the disruption of European financial networks, threat actors will eventually shift to other countries or attackers in other locales will step in to pick up the pieces. Companies recognize that the likelihood of experiencing a ransomware demand or attack is high—how they respond by identifying and containing these incidents will be critical moving forward.

'An ongoing challenge'

"It's one of those deals where I don't care how much money you throw at it. It's never going to be enough because you're just not going to completely stomp it out."

Chief Financial Officer, utilities company

Business takeover threats

Business takeover threats are among the most persistent and pervasive cybersecurity attacks on middle market companies. The attacks can be straightforward, taking the form of social engineering and employee manipulation, but their low-tech nature means they can be hard to detect. Similar to ransomware, business takeover threats require very little effort or technical skill to launch but can be very harmful to a potential victim.

With social engineering, an attacker will contact an employee directly—by phone, by email or even in person—and try to convince that person to divulge sensitive information or allow access to systems. The attacker may pose as a coworker or trusted third party to give a false sense of security. Many takeover criminals are extremely skilled in identifying and exploiting potential security awareness gaps.

However, the most common business takeover strategy is phishing. Using publicly available information, often from website profiles or social media accounts, attackers create a messaging profile that mimics a friend or coworker. While many of these attacks were, and still are, fairly crude—with easily identifiable red flags—some are increasing in complexity.

"The messages are much more powerful when they are coming from a known entity," said Ghazi. "The attacks are getting more sophisticated, and the emails are more compelling. The information appears to be coming from known vendors, and it's crafted better, with better language than ever before."

The reported frequency of business takeover attempts increased significantly in this year's data, with 58% of middle market executives indicating that outside parties attempted to manipulate employees by pretending to be trusted third parties or company executives, compared to 45% last year. Executives at smaller middle market companies reported a small increase in attacks to 53% this year from 51% in 2022, while larger companies indicated a sharp jump in incidents to 63% from 40%.

58%

of respondents said that outside parties attempted to manipulate employees by pretending to be trusted third parties or company executives, up from 45% last year.

An increase in successful business takeover attempts is a concerning trend in the middle market. Executives in the RSM survey reported that 48% of attempts to manipulate employees were successful over the last year, a considerable increase from 27% in 2022's data. Larger middle market organizations showed the largest increase, reporting a 68% success rate for attacks, compared to 38% just last year. Smaller middle market companies exhibited a small increase this year—21% from 15%.

"Employees being manipulated has increased given the diverse attack vectors that hackers can use, from the phone (vishing), email (phishing) and even text messages (smishing)," commented Ken Stasiak, RSM principal and national cyber testing and response leader.

Understandably, middle market executives believe business takeover attempts will continue to be a threat. In the MMBI study, 76% of executives said their organization is at risk of an attack by manipulating employees in the next 12 months, the highest number yet recorded in the survey and a slight increase over last year. The number of smaller organizations expecting an attack remained consistent from last year at 68%, while executives from larger organizations who believe a takeover attempt is likely increased slightly to 84%.

76%

of executives feel they are at risk of an attack by manipulating employees in the coming year.

With the potential for a business takeover attack to be launched by anybody, companies need to **employ various strategies** to discourage them. Of the organizations in RSM's survey that had unsuccessful attacks, 80% listed employees not acting on the fraudulent request as a reason for the failed breach, a 4% increase from last year's survey. In addition, 63% of middle market executives said that secondary controls prevented the completion of an attack, and 55% acknowledged system controls prevented the delivery of fraudulent communications or materials to employees.

Ultimately, training is the most effective defense against business takeover attacks, providing employees with real-life examples of how criminals commonly attempt to manipulate them. Most middle market companies understand the value of training, with 89% of executives reporting that their organization provides training to at least some employees on detecting, identifying and preventing attempts to gain unauthorized access, consistent with last year's data. Larger middle market companies appear to offer training to more employees, with 97% providing training to some or all employees, compared to 81% of smaller counterparts.

With the low level of expertise necessary, the amount of exploitable information at the disposal of attackers and constant technological advances, business takeover threats will continue to be a primary threat to middle market organizations. While companies appear to understand the threat, attack methods will continue **improving, and training strategies** and controls must advance in response.

'The biggest weakness'

"We get hit with the traditional spearfishing, malware and viruses attached to emails. And it's just a constant battle to try to stay ahead of them. The biggest weakness is always people."

Chief Financial Officer, utilities company

Privacy protections compliance

Although cybersecurity has been a key concern for middle market businesses for many years, recently, the focus has shifted with increased concern on privacy, and it will be even more of a priority moving forward, given recent marketplace trends.

Data has always been a valued commodity; however, personal data presents opportunities for middle market businesses to derive revenue-driven insights that form the basis for decision-making and the development of products and services. But with a variety of privacy requirements already in place, and with more coming soon, organizations not only have to balance protecting personal data, but also complying with laws and regulations about what information they have and how it is managed and maintained across its entire life cycle.

The dramatic shift toward an enhanced legislative and regulatory landscape for privacy and personal data began with the European Union's General Data Protection Regulation, which went into effect in 2018. This landmark privacy law and regulation established prescriptive compliance obligations for companies with personal data holdings of EU residents. These compliance obligations were further exacerbated by several high-profile enforcement actions and fines, resulting in increased attention.

The GDPR has served as a model for several subsequent laws and regulations for privacy and personal data worldwide, with additional compliance obligations eventually making their way to the United States. For many years, a federal privacy standard has been discussed in the United States. But despite significant support, momentum toward a comprehensive and industry-agnostic law and regulation at the U.S. federal level for privacy and personal data has currently stalled. Perhaps the momentum will renew with increased discussion and concern expressed over generative artificial intelligence and other technological innovations.

However, this landscape has arguably become more challenging for middle market businesses, as they must contend with a patchwork of many individual state requirements mandated by new state-level privacy laws and regulations that will only become more complex as this trend in the landscape progresses.

"We all have heard by now that 'You can have security without privacy, but you can't have privacy without security,'" said Stasiak. "However, it's turning into 'You can't have privacy without regulations.' We are seeing a significant uptick in both state and federal regulations to enforce privacy."

By the end of 2023, compliance obligations will be in place in six states—California, Colorado, Connecticut, Iowa, Utah and Virginia—with more on the horizon. There are also state-level existing and new laws and regulations that are also focused on specific personal data types, such as the health care industry and financial services.

In other words, chances are that privacy laws and regulations already apply to a company's operations at some level, so middle market businesses must understand their personal data holdings for both commercial operations (i.e., revenue-driven) and corporate operations (i.e., human resources management). Visibility and oversight of personal data holdings are the foundation for understanding and identifying compliance obligations.

In addition, for those middle market businesses with European operations, it appears that while the majority of companies understand the impacts, only 57% percent of executives in the RSM MMBI survey said they are familiar with the requirements of the GDPR. This indicates a plateau from 58% in 2022, despite increased awareness and enforcement activity. Consistent with past years, respondents from larger organizations were more familiar with GDPR requirements than those at smaller organizations—84% versus 28%.

With the expansion of privacy laws and regulations across the United States, most middle market businesses understand they will likely need to adhere to compliance obligations in the near future. Among RSM survey respondents familiar with GDPR requirements, 90% said their organizations would likely have to comply with privacy requirements similar to the GDPR at a federal or state level in the United States during the next two years, the same amount as last year.

90%

of executives familiar with the GDPR believe they will likely have to comply with similar privacy legislation at a state or federal level in the next two years.

As privacy becomes more of a priority nationwide and requirements are more complex as new state laws and regulations are enacted, middle market executives are clearly taking compliance seriously. For example, 96% of executives in the RSM survey familiar with the GDPR said preparing for emerging privacy laws and regulations is a priority, identical to last year's response.

Perhaps such statistical plateaus can be attributed to a wait-and-see approach for how enforcement activity ensues or a privacy by obscurity approach that mimics the security by obscurity approach commonplace among the responses to ransomware attacks and other cybersecurity threats.

96%

of respondents familiar with the GDPR said preparing for emerging privacy regulations is a priority.

"Nevertheless, companies will ultimately need to take action to meet their compliance obligations for personal data as privacy has become a significant business differentiator, particularly when it comes to strategic growth through innovations or mergers and acquisitions as well as third-party risk management," said Alison Brunelle, RSM senior director and national privacy services leader.

With a wave of compliance obligations spreading across the United States, managing and maintaining personal data across its entire life cycle has become even more challenging. If companies do not yet have to comply with any privacy requirements, it seems to be only a matter of time before it happens. Global expansion will likely mean compliance with the GDPR or other international privacy laws and regulations, and operational practices across multiple states will eventually require compliance with localized privacy requirements—especially as more are introduced and enacted.

Migration to the cloud to ensure data security

The cloud is an extremely valuable tool in the middle market, and almost all companies now utilize it to enhance some business functions. The initial **shift to the cloud** typically involved moving files and systems to increase access and visibility while reducing reliance on on-premise resources and servers. However, companies have also found that the cloud is an effective security tool. Due to economies of scale, cloud providers can deliver a greater depth of protection than many middle market organizations have the resources to provide.

The RSM MMBI research finds that 50% of middle market firms moved or migrated data to the cloud as a result of security concerns during the past year, up from 36% a year ago. Larger firms are showing a significant commitment to the cloud, with 65% indicating a cloud migration in the last year compared to 39% in 2022. The number of smaller middle market organizations taking advantage of the cloud remained steady from last year, up slightly to 34% from 33%.

50%

of executives reported a move to the cloud as a result of security concerns, up from 36% last year.

"People have gotten more comfortable with the cloud," said Ghazi. "A large-scale migration began in 2021 and has continued through the last two years as a key element of digital transformation initiatives."

Consistent with past years, the overwhelming majority of companies leveraging the cloud for security reasons are seeing results. Among middle market executives who reported moving data to the cloud for security concerns, 91% believe the data residing in the cloud is more secure. That represents a small increase from last year's survey (90%).

91%

of respondents that have moved data to the cloud for security concerns believe it is more secure.

While the cloud can provide a more effective security environment, it often comes at a higher cost. In this year's survey, 70% of middle market executives said that storing data in the cloud for security reasons was more expensive, a slight decline from last year's data (75%). Conversely, 27% of respondents disclosed that moving to the cloud for enhanced security was less expensive, a considerable increase from last year's data (19%).

"The cloud is attractive because you don't have to maintain internal headcount, and it's readily accessible," said Ghazi. "You also don't have to worry about upgrades and patches—that's somebody else's responsibility. However, moving to the cloud has its risks as well. The environment has to be configured properly to reap the inherent security and operational benefits. Not all subscriptions are equal, and some of the enhanced features can be costly."

The cloud provides many benefits for middle market companies, and enhanced security is one that can be extremely beneficial. While providing a more efficient, accessible environment, it can take pressure off internal security resources with a level of protection that may not be available with in-house technology deployments. It may come at a higher cost, but the enhanced protection for sensitive data and applications is a significant draw for a growing segment of the middle market.

Methodology

About the RSM US Middle Market Business Index research

The RSM US Middle Market Business Index survey data in the first quarter of 2023 was gleaned from a panel of 1500 executives (the Middle Market Leadership Council) recruited by The Harris Poll using a sample supplied by Dun & Bradstreet. All individuals qualified as 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 and financial institutions with assets under management of \$250 million to \$10 billion.

These panel members have been invited to participate in four surveys over the course of a year that include special issues-based question sets, as well as monthly index-only surveys; the 2023 first-quarter survey was conducted from Jan. 9 to Jan. 30, 2023. Information was collected by phone and online survey from 406 executives, including 183 panel members and a sample of 223 online respondents. Data is weighted by industry.

The U.S. Chamber of Commerce is a partner in this research.

Biden team makes cybersecurity a priority for government

U.S. Chamber of Commerce commentary

By Vincent M. Voci

Vice President, Cyber Policy and Operations
Cyber, Space, and National Security Policy
U.S. Chamber of Commerce

The Biden administration has adopted a strong, proactive approach to cybersecurity policy, recognizing the urgency of protecting the United States from cyberthreats. And for good reason: In 2016, Russian-backed actors conducted intrusions into U.S. political institutions; in January 2021, the United States faced significant cyber risk when a Russian government-backed operation breached the SolarWinds Orion network management software. In response, the Biden administration launched a 100-day sprint to strengthen the cybersecurity of the nation's industrial control systems for the electricity sector. President Biden also signed Executive Order 14028 on Improving the Nation's Cybersecurity in May 2021 to safeguard the software supply chain.

EO 14028 requires the U.S. government to define public security measures for critical software, uses the government's purchasing power to drive enhanced cybersecurity standards into IT systems purchased by the government, and articulates a vision for zero-trust architectures in federal government networks. Another key aspect of the administration's cybersecurity policy is the focus on addressing ransomware, with the administration publicly vowing to hold ransomware actors accountable.

Congress has passed several notable pieces of legislation, including the Cyber Incident Reporting for Critical Infrastructure Act of 2022, or CIRCIA, which established a mandatory cybersecurity incident reporting program. The U.S. Chamber of Commerce was influential in the congressional negotiations around CIRCIA, advocating for its members' priorities across timelines, covered entities, substantial incidents and legal liability issues.

The Biden administration's National Cyber Strategy articulates the whole-of-government, whole-of-society approach to rebalancing responsibilities for defending and securing cyberspace. The NCS communicates a new direction for cyber policy in the United States, starting with the premise that voluntary industry and market forces have failed to adequately invest in cybersecurity, risk management and resilience. Therefore, regulation is required to incentivize industry investment in stepped-up cybersecurity.

Cybersecurity best practices for organizations have remained uniform for years, including risk assessments, security measures, incident response and employee training. However, as the U.S. Chamber found in a [recent report](#), regulation has dramatically increased over the last decade. Midsize businesses should monitor regulations along four categories of cyber public policy risk, including sector-specific cybersecurity regulations (e.g., [TSA rail and pipeline](#), [EPA Public Water](#)), [incident reporting](#) or [public disclosure](#), common cybersecurity standards (e.g., [NIST Cybersecurity Framework](#), [CISA Performance Goals](#), [CISA Security-by-Design and -Default](#)), and state-by-state approaches to cybersecurity regulations (e.g., [State of New York Legislation A.3904B/S.5579A](#)). Given that cyber risk from threat actors has steadily increased over the same period, according to the U.S. Chamber's analysis, there is a significant growing risk to businesses from public policy, such as changes to laws, regulations or legal enforcement.

While there is a growing willingness by both political parties in Washington to pursue aggressive policy changes through regulation, the U.S. Chamber is committed to working alongside policymakers to ensure that good intentions do not lead to undesirable policy outcomes.

The shift toward managed security services in the middle market

Managed services strategies have been key to the success of many middle market companies for years, delivering additional resources and valuable experience while supplementing internal personnel when and where organizations need it. Managed services have historically been associated with technology tools and applications, but now the approach includes IT security services, which offer similar advantages for companies.

The business world is becoming more digital every day, and with increasing employee and customer expectations, companies cannot risk being left behind. That influx of innovation has created a considerable amount of strain on the internal resources of middle market companies. In many cases, organizations do not have in-house experience managing emerging tools and platforms, leading to potential cybersecurity gaps.

In addition, the rise in digital deployments and a tight labor market have created an environment for qualified talent in which many middle market companies find it difficult to compete. Or, if personnel can be brought in, they are difficult to retain. A revolving door of never-ending hiring, training and transferring the right knowledge to new personnel is often costly and counterproductive.

"In the middle market, some organizations have zero IT people on staff, and some have a few, but not enough to cover their entire environment," said Steve Kane, RSM director and managed security services lead. "Paying whatever the market demands for them and then training them, keeping them up to date on emerging trends and threats on top of needing to spend on tools—it often becomes too costly. It's too much upkeep when there's already proven solutions in a managed security setting."

Managed security services come in many forms. Strategies can either be deployed in-house or remotely, providing advanced resources for critical areas, including monitoring, patching and advanced threat detection and response. Managed services providers typically have access to a higher level of tools, insight and experience than middle market companies can typically take advantage of internally.

For example, RSM Defense is RSM's managed security services platform, with military-grade tools and advice from experienced professionals. The platform's goal is to block an adversary's advantage with solutions that include embedded machine learning algorithms to detect anomalies within a business environment and artificial intelligence to rapidly discern friend from foe and initiate the necessary response.

"Middle market companies want solutions that address their needs in a cost-effective manner," commented Daniel Gabriel, RSM principal and North American cyber transformation lead. "They do not have the time or the people to deal with refreshing hardware or staying on top of the latest trends. They are looking for a one-stop shop with a reliable cost structure to make problems go away."

Incorporating a managed security services component into a company's security program provides inherent flexibility. The organization can adjust the scope of services based on specific needs, scaling up or down quickly to adapt to changes in business objectives.

"If a company has a monitoring problem, a service can deal with that," said Gabriel. "If they have identity management problems, a service can help them there as well."

A managed solution is also not an all-or-nothing proposition. Companies have access to necessary resources to support their security strategy, and providers can work hand-in-hand with existing internal personnel as a vital component of their team. In these situations, having a single provider that can help a company consume an expansive set of managed services adds efficiency and scalability not only from a cost perspective but also from the service synergy and cohesiveness perspective that companies should expect.

Gabriel outlined how that scenario commonly works. "If you already have people on staff, you can elevate their role a bit more," he said. "If they have a background with a specific tool or activity, they could become the coordinator with the third party," he said. "Or they could become an expert-level individual who receives information when an issue is identified and acts upon it. It allows the organization to get more value out of its people."

With the continued deployment of **digital technology**, the need for managed security services will continue to grow. The combination of cost containment, flexibility, leading tools and advice will become a pillar of more middle market cybersecurity strategies in the future.

For more information on RSM, please visit **rsmus.com**.

For media inquiries, please contact Kim Bartok, national public relations director,
+1 212 372 1239 or kim.bartok@rsmus.com.

For more information on RSM thought leadership, please contact Deborah Cohen,
thought leadership director, +1 312 634 3975 or deborah.cohen@rsmus.com.



www.rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM, the RSM logo and *the power of being understood* are registered trademarks of RSM International Association.

© 2023 RSM US LLP. All Rights Reserved.

