RSM US MMBI Special Report: Cybersecurity 2024

This special report on cybersecurity from the RSM US Middle Market Business Index provides insights into cybersecurity trends, strategies and concerns shaping the marketplace for midsize businesses in an increasingly complex risk environment.

TABLE OF CONTENTS

Executive summary

Rising breaches reveal ongoing cybersecurity challenges in the middle market

Key takeaways:

1. Reported cybersecurity breaches in the middle market have tied a record high in RSM's research.
2. Reasons include complacency and emerging technology such as AI.
3. Smaller firms lag in budgets and staffing, as well as in leveraging technology to address threats.

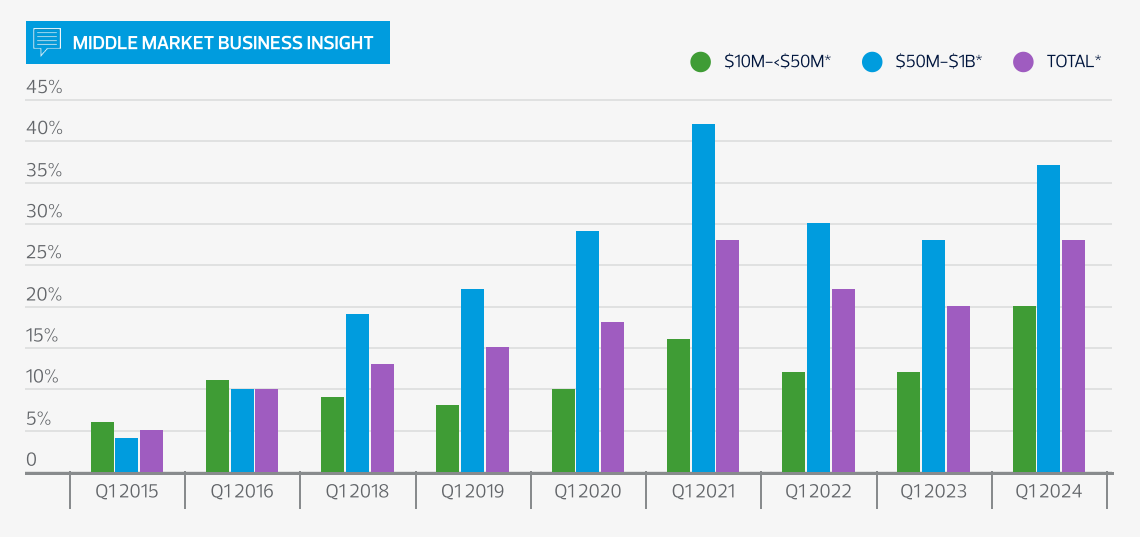
Cybersecurity remains a critical concern for middle market businesses. According to RSM data, reported breaches over a recent one-year period matched a high seen only once before in nine years of data collection by the firm. The threat environment is more challenging now as generative AI and other new technologies increase risk, placing an enterprise emphasis on well-maintained protective strategies.

Twenty-eight percent of middle market executives surveyed in the Q1 RSM US Middle Market Business Index survey said their organizations experienced a data breach in the last year, rising from 20% in the 2023 survey and matching 2021 results. Increases were seen across the board, as breaches at smaller middle market companies rose to 20% from 12% a year ago, and those at their larger counterparts were up to 37%, compared to 28%.

Even as breaches were up, 95% of survey respondents are confident in their current security measures. This year's survey also saw a record-high number of companies that carry a cyber insurance policy (76%) and respondents that made a move to the cloud due to security concerns (55%). But while 37% of executives said cybersecurity will get an increasing share of the organization's revenue, 61% of middle market decision-makers have two or fewer dedicated data security or privacy employees.

The MMBI survey, conducted online from Jan. 8 to Feb. 16, 2024, on behalf of RSM by The Harris Poll, drew responses from 403 middle market executives across a variety of industries. Survey research provides insights of those at smaller ($10 million to less than $50 million in revenue) and larger ($50 million to $1 billion in revenue) middle market organizations; in many cases large gaps exist between the two groups. The data shows that smaller middle market firms lag their larger counterparts in budgets and staffing, as well as in confidence in implementing, generating value from, and using technology to address threats.

Experienced a data breach in the last year



Source: RSM US Middle Market Business index, Q1 2024

*TOTAL: Q1 2015 (n=148), else (n=399-424); $10M-<$50M: Q1 2015 (n=78), else (n=167-217); $50M-$1B: Q1 2015 (n=51), else (n=172-198)

RSM risk professionals cite complacency, the rapid adoption of emerging artificial intelligence technology and threats from foreign actors as among the worrisome trends responsible for the recent sharp uptick in cyber incidents.

"In working with clients and customers, there has been a fatigue with cybersecurity," says Tauseef Ghazi, an RSM principal who leads the firm's cybersecurity practice. The behavior harks back to the two-year period after the pandemic began, he says, adding: "We are not quite at that point, but we are dangerously close to it."

Meanwhile, Ghazi notes that breaches are larger, with more widespread and deleterious effects on businesses. "They require a lot of time and effort to recover from," he says.

Add to this mix AI technology. Broadly lauded for its ability to bolster innovation and wring efficiencies from mundane processes, AI has also become a tool in cybercriminals' arsenal. When put to ill use, the technology's algorithms can make short work of illegal sleuthing that leads to attacks, he says.

"AI is not only available to the good guys—it's available to the bad guys as well," Ghazi says. "What they could do in an hour before, they can do in seconds now."

RSM Principal David Llorens emphasizes how cybersecurity threats continue to expand. "A lot of companies that have never been targeted before are being targeted now," he says. "And many of the cyber events that we see are from threat actors that sit in countries not friendly with the U.S."

Middle market insight

"In the past it has always been the large corporations that hackers have gone after. Now they're going after the medium and smaller-size companies."

Executive, consumer products

At the end of the day, most attacks are based on opportunity. Hackers are relentless and will work to find vulnerabilities to exploit within a company's network, an entire industry or a broader ecosystem, says Matt Franko, an RSM principal.

"Hackers are like water," Franko says. "They will flow to where they think they can get money, just like any other business."

The unpredictability of potential attacks and the broad range of threats to sensitive data and intellectual property require companies to remain ever vigilant. Attacks are occurring more often and becoming more expensive, and they can be very harmful or even fatal for companies with tight profit margins. Any disruption in operations has a direct impact on profitability; the longer an issue persists, the more difficult recovery becomes.

Companies must ensure that controls are up to date and protective measures are leveraged to take a proactive stance in the ongoing battle against cybercrime. They must improve their cybersecurity program and strategy, focusing on:

- Asset management
- Digital identity
- Data governance and security
- Third-party risk management
- 24/7 detection and response (often supported by managed security services)
- Regulatory and compliance requirements (typically using a governance, risk and compliance tool)
- Risk-based operational resilience

Explore cybersecurity trends by industry

No matter the industry, cybersecurity is a critical consideration for ongoing success.

View your industry

Cyber breaches trend lower in UK, as investment rises

Unlike in the United States, where cyber breaches tied an all-time high for middle market companies in the past year, attacks are trending lower in the UK over the same time period. Twenty-one percent of executives in the Q1 RSM UK MMBI survey indicated their business experienced a breach, down from 27% two years earlier.

88%
Said their business increased cybersecurity investment in the past year, up from just over half (52%) in the first quarter of 2022.

94%
Said their organization was somewhat prepared or very prepared for a cyberattack.

50%
Had plans in place to tackle compliance with impending cyber regulation such as NIS2.

Cyber budgets are on the rise for many companies

As risks evolve, staffing strategies may also require attention

Key takeaways:

1. More than a third of middle market managers reported increasing the amount of revenue dedicated to cybersecurity in the coming year.
2. More than 60% of executives have two or fewer internal security and privacy employees.
3. Budgets most often reside under the chief technology officer or chief information security officer.

Cybersecurity events can result in significant financial repercussions, reputational harm and operational chaos, making it imperative that middle market companies allocate sufficient budget and staff to effectively address threats. While the RSM MMBI data finds that many organizations are increasing budgets, concerns over staffing and how funds are allocated could limit the effectiveness of cybersecurity efforts.

Survey data shows that 37% of the middle market executives overall will increase the proportion of their organization's revenue devoted to cybersecurity in the upcoming year. But more funding may be necessary to address the cybersecurity threat at smaller organizations, as just 29% of managers from smaller companies planned to increase the amount of revenue dedicated to cybersecurity, compared to nearly half of larger middle market companies (48%).

Spending more does not necessarily ensure an effective strategy, RSM Principal Matt Franko cautions. "During COVID, many companies bought a lot of tools, and many of those had overlapping and redundant uses," he says, adding that many companies are still seen as tool heavy right now, but may lack the right people and processes in place to take advantage of those investments.

Middle market insight

"To set up the infrastructure, to catch it before it starts doing damage, is pretty much cost prohibitive. The cost is in the five figures a month to keep it from happening."

Executive, consumer products

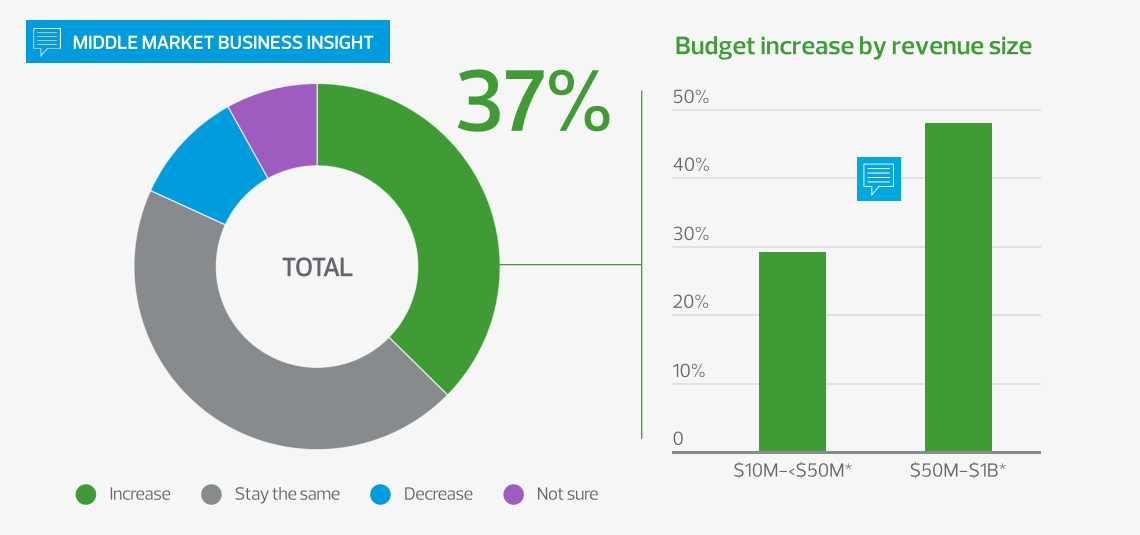
Budgetary control is an important element in how a cybersecurity strategy is built. Companies emphasize cybersecurity in different ways in the middle market, and therefore, internal funding sources for the function can vary greatly.

The MMBI survey showed cybersecurity was most commonly located under the chief technology officer (51%) or the chief information security officer (42%), according to respondents whose companies had a dedicated function focused on data security and privacy. The report also showed that 34% of companies had cybersecurity budgets under the chief financial officer and 32% residing under the chief executive officer.

"Cybersecurity needs to have a dedicated budget because it's a risk management function and oftentimes gets sacrificed over other priorities," says Franko, who favors alignment under the CFO. "You only have so much money to spend, and you have to determine whether you are going to spend it to make money or protect yourself from losing money."

From a staffing perspective, more than 60% of respondents have two or fewer data security and privacy employees. Not surprisingly, larger middle market organizations have more dedicated internal staff; 40% of those respondents have four individuals or more. Meanwhile, 27% of smaller middle market companies—the largest response in that subset—cited no internal personnel, but instead leverage external providers for data security. Another 7% of smaller middle market companies have no internal personnel and either are considering creating a dedicated function (3%) or are not considering creating a dedicated function (4%).

Cybersecurity budget—expected change next year



Source: RSM US Middle Market Business index, Q1 2024

*$10M-<$50M (n=189); $50M-$1B (n=198)

Within many companies, the question isn't always about the number of people, but whether they are the right people for the job. In the last decade, companies have become much more dependent on technology, but IT departments may not have kept up with the change.

"Even if products and services are not tech-focused, technology is the highway the business runs on," says RSM Principal David Llorens. "The moment you block that highway, the business is crippled. You then cannot trust data and you cannot effectively work with clients and customers because everything is interlinked."

In more recent years, COVID-19 disrupted companies and pushed them to transition to a remote workforce, decentralizing control and effectively creating a larger attack surface.

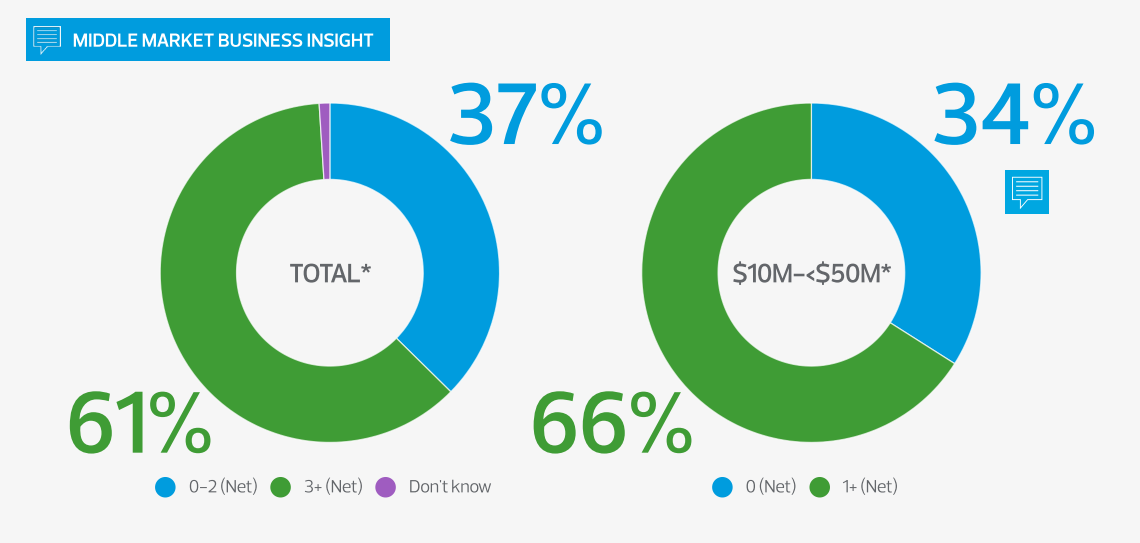
"Companies adopted cloud and software-as-a-service strategies, but they have the same IT team," Llorens says. "They may not understand how the data flows after having adopted the new technology."

RSM Principal Tauseef Ghazi has observed skill gaps in internal IT departments. "Technology has advanced so much and become essential to every area of the business," he says. "But in many cases, the internal skill set is not growing to match new technology."

Meanwhile, in a competitive environment for skilled workers, cybersecurity personnel are difficult to hire and retain, a major factor Llorens cites when advocating for under-resourced companies to consider managed services strategies and other external support.

"There often is a knowledge gap where IT may not understand how to protect their environment—this is the direct value vendors and managed services firms can provide," he says.

Number of data security/privacy employees



Source: RSM US Middle Market Business index, Q1 2024

*TOTAL (n=402); $10M–<$50M (n=189); $50M–$1B (n=197)

Are you confident in your overall cybersecurity approach?

Learn how to better identify security risks, incorporate security into your business processes and make more informed business and risk decisions.

Address your security needs

Executives confident in cybersecurity measures

Despite optimism, resource gaps and a lack of optimization can limit effectiveness

Key takeaways:

1. Confidence in current cybersecurity strategies remains high (95%).
2. 76% of middle market managers carry a cyber insurance policy and 75% of those are familiar with their coverage.
3. Large gaps exist between how small and large firms leverage technology to address threats.

Most middle market businesses appear to be taking risks seriously. While the strength and scope of cybersecurity strategies are steadily progressing, some vulnerabilities and opportunities remain.

Despite the rise in reported cyberattacks in the MMBI data, the number of respondents confident in their existing strategies remains high. In fact, 95% of middle market executives reported they are either very confident or somewhat confident in current measures to safeguard data, tracking closely to the 96% in both the 2022 and 2023 data.

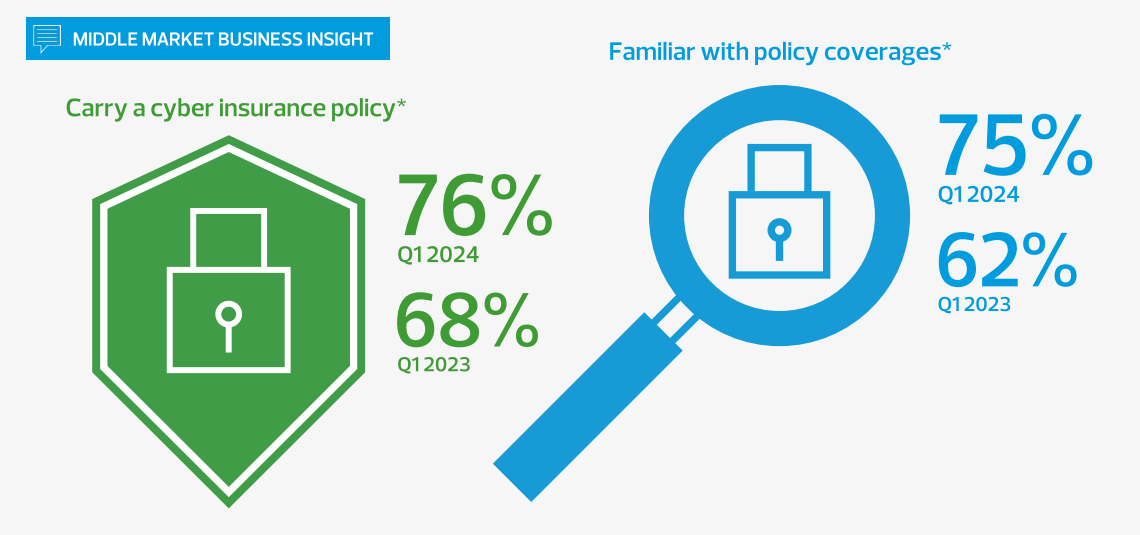
RSM Principal Tauseef Ghazi asserts that complacency may be a factor in that confidence, fueled in part by a false sense of security from having more information about incidents at executives' disposal. "It's not that breaches have gone away," he says. "They have just become part of life, and often, someone else is taking care of them. Also, in the last year or so, when some people got compromised, they thought, 'OK, we are fine, we will be back up and running in five days.' But some organizations weren't fine."

Responding to a breach can be expensive and labor intensive, and cyber insurance is one of the most popular measures organizations employ to protect themselves. Many policies have undergone significant changes in recent years, as insurers responded to rising costs by increasing premiums, reducing coverage limits and requiring certain cybersecurity measures by organizations before issuing policies. Even after these changes, cyber insurance is still one of the most effective tools companies have.

"Cyber insurance carriers almost act as a governing body by requiring certain controls," says RSM Principal Matt Franko. "Companies need to make sure they are covered because nobody wants to get hit with an attack that costs them more money than necessary."

He adds: "That would be a tough thing to tell the board or shareholders—that we just didn't have the coverage because we didn't implement the necessary controls."

Companies that carry cyber insurance and familiarity with coverage



Source: RSM US Middle Market Business index, Q1 2024

*Carry a cyber insurance policy: Q1 2023 (n=406), Q1 2024 (n=403); Familiar with policy coverages: Q1 2023 (n=308), Q1 2024 (n=278)

Cyber insurance use is trending up in the middle market, as more than three-quarters of respondents in the MMBI survey (76%) indicated they carry a policy. This represents a significant increase from 68% in last year's survey, and an even bigger jump from 61% just two years ago. Eighty-three percent of larger middle market companies reported having an active policy, up from 70% last year, while use in smaller middle market companies lagged slightly, rising to 72% from 67% in 2023.

Perhaps most importantly, understanding of coverage is increasing. Seventy-five percent of survey respondents carrying a policy indicated they are familiar with their policy, up from 62% last year. In fact, 52% of companies said they are very familiar with their coverage, a surge from just 22% in 2023.

"Each year the policies change," says Daniel Gabriel, a principal at RSM, noting the resulting confusion. "So, the biggest thing, especially for middle market organizations, is understanding the limitations and expectations of policies. Many people buying cyber insurance may not completely understand their policy and what the implications are, and they may be losing coverage every year."

Turning to preventive technologies, MMBI survey respondents had varying opinions on how cybersecurity tools are deployed within their organizations. Eighty-six percent of middle market executives rated their use of technology as excellent or good, while 82% said the same about their technology implementation, and 74% shared that sentiment about the value their tools generate.

However, significant gaps in confidence over tools exist between larger and smaller middle market organizations. Ninety-four percent of respondents at larger middle market firms said their use of technology to prevent or minimize threats is excellent or good, compared to 79% at smaller organizations. This disparity was even wider when the survey tracked positive feelings about implementing technology (93% vs. 73%) and generating value from technology (88% vs. 60%).

"Many tools are excellent, but they are often not optimized," says Ghazi. "To be truly effective, tools must be tailored for a company's environment, data, and the types of alerts and preferences they require." For example, if an advanced governance, risk and compliance (GRC) tool does not have effective workflows built in, it will not operate as intended."

Whatever their size, companies need to focus on the effective implementation and operation of technology solutions, especially as options such as GRC tools gain traction as a valuable defense against cybercriminals. Several emerging solutions can automate GRC efforts, bringing more consistency, efficiency and insight to the process.

The need to maximize investment in modern, effective security tools is another factor leading companies to **consider managed security services** strategies for their cyber defenses, especially in the lower middle market.

"The cost of tools is hedged across multiple clients in many cases, making a higher level of protection much more affordable," says Ghazi. "Benefits also emerge with personnel costs, because an analyst can monitor 20 clients at the same time with advanced automation, rather than a company hiring one person to manually monitor their environment.

Digital identity measures in the spotlight

The security perimeter is expanding—identity strategies must shift accordingly

Key takeaways:

1. Strategies must constantly evolve, especially as digital identity becomes more complex.
2. Providing access as needed is the most popular identity strategy, but may present challenges.
3. Only 11% of respondents said password use is outmoded, representing a major opportunity for improved security.

The network no longer represents the security perimeter; instead, identity is the new perimeter. As customers, employees and service providers engage more often with companies' digital systems and hackers constantly try to break in, controlling information access is critical. The concept of **digital identity** helps organizations build profiles of characteristics of employees, customers, third-party users, programs and organizations to determine what, if any, access they should have.

An effective **digital identity strategy** must constantly evolve as new users and groups require access and some existing users no longer do, and as new strategies become available to verify users and their purpose. The right approach can protect sensitive data and improve the online experience for both customers and employees.

MMBI data indicates that middle market companies are in various stages of their digital journey, with 31% of executives saying their companies provide people with access as needed. In addition, 24% provide single identity solutions such as single sign-on for system access, while another 22% require disparate usernames and passwords.

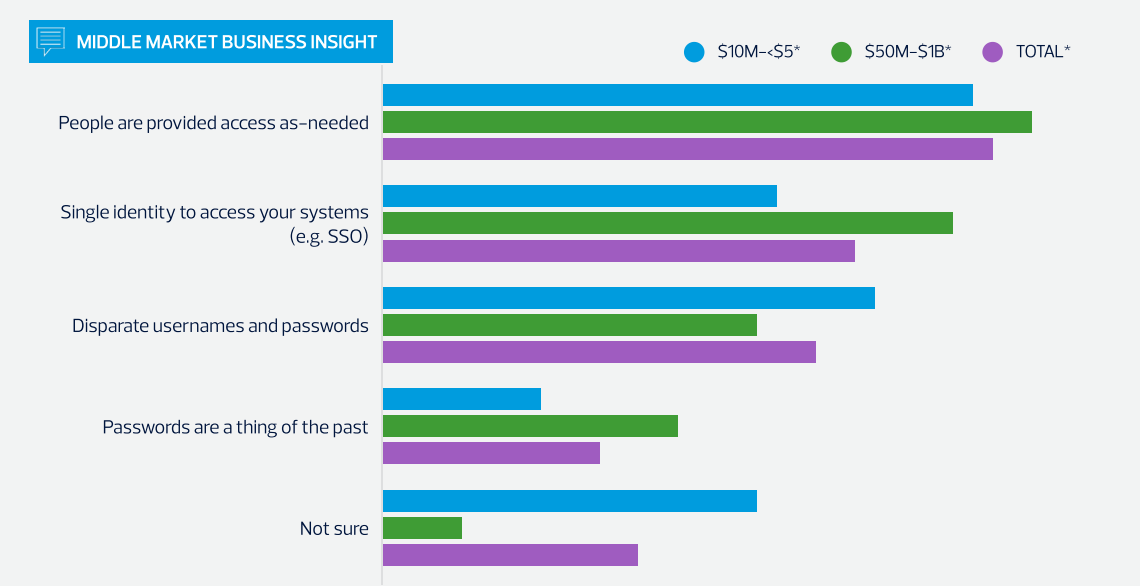
"By providing access as needed, provisioning and deprovisioning access can be a nightmare," says RSM Principal Tauseef Ghazi, noting that access privileges must be removed when no longer needed—in effect, provisioning and deprovisioning to ensure users only have access to necessary systems and applications.

"Usually, users aren't telling you they no longer need access," he says.

RSM Managing Director Chad Wolcott adds that the use of disparate usernames and passwords can result in a more secure environment but comes with a cost: a less seamless user experience.

"In some respects, having disparate usernames and passwords limits or minimizes your threat vectors," he says. "If someone gets a credential, they can only access that area—versus a single sign-on approach where if someone gets that credential, they have access to everything that person has rights to."

Digital identity measures



Authentication measures that don't require passwords represent the future of data security, tying identity to specific users and/or devices and providing confirmation, typically through text messaging, email or biometrics. Even so, just 11% of executives in the RSM survey said their digital identity journey is this mature, with passwords a thing of the past.

This leaves significant opportunity to improve the user experience in the middle market, where businesses must balance their users' desire for easier access with their own need for leading-edge security. Fortunately, identity and access management (IAM) strategies can deliver both.

Passwords are inherently vulnerable and can be relatively easily compromised in a number of ways. As threats persist, companies should work toward eliminating passwords from their environment as much as possible and creating a stronger, more user-friendly data security approach.

"We are definitely seeing a move toward passwordless authentication, especially from those who are focusing on their employee and customer user experience by not having to remember lots of passwords," says Wolcott. "So, you don't have to maintain the password—instead you may just pick up your phone and look at your face ID to gain access."

Middle market must resist complacency amid persistent ransomware and third-party risks

Monitoring and response capabilities are critical to counter risks

Key takeaways:

1. Ransomware attacks are holding steady, and remain a significant threat.
2. 41% of respondents from larger firms experienced at least one attack last year, compared to 21% of smaller firms.
3. Just over half of executives surveyed reported using governance, risk, and compliance or other tools.

Ransomware remains a widespread concern in the middle market, with attacks that can force specific systems, business units or entire companies to grind to a halt. The repercussions vary, ranging from financial losses and penalties to reputational damage, as well as opportunity costs if some functions become inoperable and a company is compelled to shift resources to recovery efforts.

Thirty percent of middle market executives surveyed in the MMBI reported having at least one ransomware attack or demand in the previous 12 months. This represents a small decrease from 35% in last year's survey, but a 7% increase from 23% two years ago. Other leading cybersecurity research, including from NetDiligence, indicated consistent or increased ransomware activity in the last year, emphasizing the persistent threat.

With ransomware attacks remaining prominent in the middle market, companies cannot afford to lose focus. Incidents may not be as prevalent in the news cycle as in the past, but that does not make them less harmful.

"Everyone has gotten numb to ransomware," says RSM Principal Daniel Gabriel. "But as international conflicts subside, it is going to be interesting to see what happens when groups and individuals no longer have that focus. They are going to turn around and start evaluating opportunities in the rest of the world."

Larger middle market companies are a more popular target for hackers looking to collect ransom, with 41% of executives from those organizations reporting at least one attack or demand in the last year, compared to 21% of respondents at their smaller counterparts. However, that same subset of larger companies actually reported a 13% decrease in ransomware threats compared to last year, while smaller companies saw an 8% increase.

Middle market insight

"Every day, multiple times a day, we get phishing emails. It's a constant reminder for us to stay vigilant about where emails come from and to not click on anything—just delete, delete, delete."

Executive, manufacturing

"Larger companies are spending more money on cyber, and monitoring controls have gotten better," says RSM Principal Tauseef Ghazi. "But this is another connection point to a managed services strategy. It is hard to maintain the necessary monitoring to identify ransomware the minute it hits. You only have seconds, maybe minutes—not hours—to move it to quarantine and contain it."

For companies that reported at least one attack in the last year, 28% said existing security measures were unsuccessful, 32% said they were partially successful and 40% said they were completely successful. Interestingly, the survey data showed very little difference in the success of ransomware defenses between smaller and larger middle market companies.

"There is really no material difference in the results for the organizations that have much higher spend and higher head count," says RSM Managing Director Chad Wolcott.

Gabriel suggests that a change in ransomware strategies may be in order. "It's much better to invest in the ability to rapidly detect, respond and recover than it is to protect," he says. "It's more important to get your company back up and running quickly, and then deal with the rest of the chaos. By resuming operations and making money again, you can at least pay for the chaos. But the pivot to that mentality hasn't fully occurred, especially in the middle market."

Many ransomware attacks are the result of vulnerabilities within third-party risk strategies. RSM survey data shows opportunities for middle market companies to improve those controls. For example, almost two-thirds of respondents (64%) regularly evaluate the cybersecurity controls of third parties and nearly 3 in 5 (58%) include service-level agreements and other data and security controls in contractual agreements.

In addition, just over half (53%) of the survey respondents use a governance, risk and compliance (GRC) or other tool to manage third-party risk management, half include critical third parties in business continuity and disaster recovery planning, and only 39% maintain a vendor inventory with vendors classified in accordance with a defined risk matrix. Implementing any—or a combination—of these strategies can mark a significant step toward mitigating potentially harmful third-party risks.

How proven is your process?

As business processes become more complex, companies often rely on specialized contractors and third-party service providers to focus on core activities. However, this practice comes with a certain level of risk. Learn how to address the introduction of various levels of vendor risks.

Address your key risks

Challenges and opportunities in the complex data security and regulatory environment

Companies must keep an eye on operations as new standards emerge

Key takeaways:

1. U.S.-based companies face a complex patchwork of data privacy regulations.
2. 90% of executives cited preparing for emerging privacy legislation as an important priority.
3. 65% of respondents are familiar with Cybersecurity Maturity Model Certification regulations.

Since the European Union introduced its General Data Protection Regulation (GDPR) in 2016, several subsequent industry and state-specific data privacy standards have shaped how organizations collect, store and share personal information. There is currently no federal data privacy standard in the United States; instead, organizations operating across multiple states must contend with a patchwork of varying regulations.

That patchwork consists of regulations in 15 individual states; in 17 other states, privacy regulations are at various stages in the legislative process. RSM Director Laura Gomez-Martin sees both positives and negatives to the assortment of state-level privacy laws.

"The good thing is that most of these regulations have common principles and a lot of the same general language," she says. "However, there are some nuances. For example, your company might be big enough to qualify as an entity that needs to comply with a law in one state, but not big enough under another state's law. Domestically, companies really need to understand their operational footprint—where they sell their goods and services and where employees are based."

Of course, companies with international operations must comply with security standards, such as the GDPR, where they do business.

"A lot of major countries already have established privacy laws, so we are not seeing as much of an increase in the regulatory landscape internationally," says Gomez-Martin. "But as companies grow internationally, they still need to take those central factors into account—where they are selling their goods and services, and where employees are based."

Gomez-Martin also cautions companies about some of the **regulations** that dictate oversight on data collected and transferred internationally, especially when information moves from one company to another. Many international frameworks require data to stay within certain geographical limits or require contracts to transfer it outside of those limits, she says, adding: "That is a huge concern internationally that may not affect companies that only have domestic operations."

Amid the challenging regulatory environment, 90% of middle market executives in the MMBI survey cited preparing for emerging privacy legislation as an important priority—but that figure is a 6% drop from last year and the lowest level in survey history. Ninety-six percent of executives at larger middle market companies consider privacy a priority compared to 86% at smaller middle market organizations.

"The drop we see is probably due to not having a new regulation that is driving the focus," says Charles Barley Jr., a principal at RSM. "But that does not mean those organizations are saying privacy is any less important. They still have the ongoing risk management responsibilities and the expectation to truly protect what we call the digital asset—what makes them 'them,' but in an electronic form."

From a regulatory compliance perspective, the Cybersecurity Maturity Model Certification (CMMC) is a critical standard for U.S. companies that do business with the federal government. In response to the need for enhanced security measures, the U.S. Department of Defense introduced CMMC guidelines to enforce the security expectations that contractors and subcontractors in the defense industrial base are required to maintain to protect controlled, unclassified information.

"If you've been a defense contractor since 2016, the Department of Defense already stated its expectations in any contract that you signed," says Barley. "CMMC is just a vehicle that is placed on top of that requirement to prove through an independent verification arm that you are doing what you already signed up for. It's similar to Sarbanes-Oxley, when CFOs were forced to attest that they built internal controls to support the accuracy of what was shared in the market."

Sixty-five percent of middle market executives surveyed said they are familiar with **CMMC regulations**. However, 85% of executives at larger middle market companies indicated they were familiar with the emerging standard, compared to just 48% of those at smaller organizations.

The DOD recently proposed a CMMC final rule—known as CMMC 2.0—with enforcement scheduled to begin in early 2025. But companies should not wait to implement new guidelines, as they represent cybersecurity best practices and being prepared will make working with the federal government a smoother process once the standard goes into effect.

"If organizations reduce CMMC to just a legal compliance activity, they're forgetting the importance of what it was really designed to do," says Barley. "The entire DOD cyber expectation is designed to help all the suppliers protect national security—whether you are a retail company that helps troops have a similar lifestyle if they are at home or abroad protecting our liberties, or a manufacturer that produces the engine or the jet fuel that goes into F-35 fighters."

Even If companies are not currently working with the U.S. government, becoming a contractor should be a consideration for growth. Federal contracts are very lucrative for many middle market companies, and they represent a consistent source for sales and can open the door to many other potential sales opportunities.

Barley emphasizes the potential benefits of working with government entities. "The federal government will always be there," he says. "I would never say it's truly recession-proof, but they always have to find a way to provide services to execute our national security strategy."

Timeline of cybersecurity and data privacy regulations*

MIDDLE MARKET BUSINESS INSIGHT

2018	2020	2023	2024	2025	2026
• EU General Data Protection Regulation (GDPR)	• California Consumer Privacy Act (CCPA)	• California Privacy Rights Act (CPRA) • New privacy laws effective in four U.S. states	• EU Network and Information Security Directive (NIS2) • New privacy laws effective in three U.S. states	• Cybersecurity Maturity Model Certification (CMMC) 2.0 • New privacy laws effective in six U.S. states	• New privacy laws effective in two U.S. states

Source: RSM US Middle Market Business Index, Q1 2024

*As of May 8, 2024

Are your compliance obligations aligned?

Balancing business risk with business needs has become more challenging as organizations face more complex regulations and standards. Learn how to simplify risk and compliance with strategies that align with your overall business goals.

Optimize your enterprise risk management

Confidence in the cloud

Companies continue the move off premises for data security

Key takeaways:

1. 55% of middle market companies moved to the cloud as a result of security concerns, a record high in RSM's research.
2. 65% of larger organizations moved to the cloud, compared to 45% of smaller companies.
3. 89% of respondents feel more secure with their data in the cloud.

Momentum to migrate corporate data to the cloud has not slowed, as companies continued to move data and systems off premises to increase cybersecurity protections. While companies still retain ultimate responsibility for data security, cloud providers often have more extensive security capabilities due to their economies of scale.

The MMBI survey data indicates that middle market companies continue to take advantage of the cloud. Cloud migration as a result of security concerns was at its highest level (55%) in MMBI survey history, up from 50% last year. Migration for smaller (45%) organizations also reached its highest level, and the share of larger (65%) organizations that made the move matched last year's record high.

"Use of the cloud for security purposes is getting normalized, and as it does, companies feel like the tools they are getting are more secure," says RSM Principal Tauseef Ghazi.

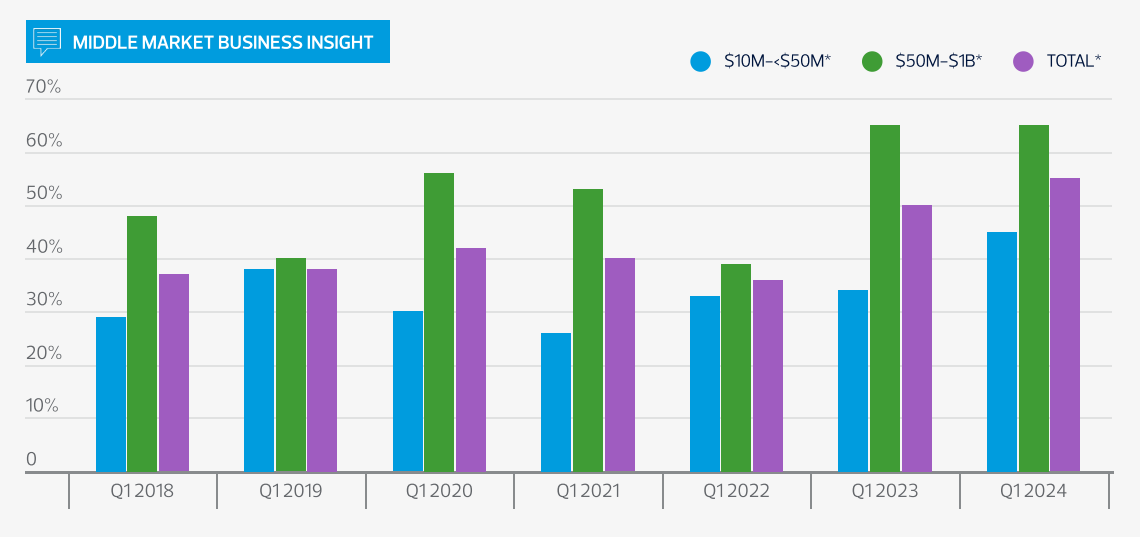
Most importantly, the move to the **cloud for security** reasons appears to be successful, as 89% of survey respondents said they felt more secure with their data in the cloud. Larger middle market companies appeared particularly confident, with 62% of executives indicating they were much more secure, up 22% from last year's survey and reaching the highest level ever.

Despite the confidence in the security of cloud-based systems and data, companies still need to be careful to ensure their assets are sufficiently protected, especially after an initial move to the cloud.

"While these established cloud platforms have a ton of security tools and products, by default, none of that is activated," says RSM Principal Daniel Gabriel. "Organizations struggle with understanding what is already active and what they have to turn on, and that can have cost implications. Companies need to turn on or opt into security options, and they may not understand the details when they first move onto these platforms."

In addition, even in a cloud environment, companies need to remember that they are still ultimately responsible for the security of their proprietary data.

Migration to the cloud as a result of security concerns in the past year



Source: RSM US Middle Market Business Index, Q1 2024

*TOTAL (n=399–412); $10M–<$50M (n=166–213); $50M–$1B (n=172–224)

Is your cloud strategy truly effective?

Is your cloud strategy truly effective? Learn more about how you can leverage the cloud for more access and enhanced security.

Move ahead of the competition

Industry perspectives on cybersecurity

Financial services

The financial services industry is among the most attractive to cybercriminals: Consider the potential financial gain of mining enormous amounts of personally identifiable customer information and an endless volume of monetary transactions. From banks to insurance companies, businesses in this space have access to a plethora of documents with highly sensitive customer information, says Angela Kramer, an RSM financial services senior analyst.

"Financial institutions are heavily reliant on digital platforms, and consumers who need to originate a loan for a car or house typically do it through a software program or online," says Kramer. "That amplifies the complexity of cybersecurity threats, and risk leaders need to help mitigate that complexity."

Over the last year, regulators have introduced new cybersecurity rules requiring institutions to elevate their standards to bolster protection against such threats. Such regulations include the U.S. Federal Trade Commission's amendment to its Standards for Safeguarding Customer Information, which requires all nonbanking financial institutions to report a data breach incident within 30 days after discovery if it involves the information of at least 500 consumers. That **Safeguards Rule update** will take effect in May 2024.

The U.S. Securities and Exchange Commission also adopted rules **in July 2023** that require all public companies to "disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance."

As cybersecurity threats constantly evolve, banks and other financial services companies continue to adapt, fortifying their own defenses while addressing risks involved in working with vendors and other third parties.

"Most insurance companies are looking at mitigation strategies focused on technology as well as policy improvements," says Marlene Dailey, an RSM financial services senior analyst focused on the insurance space. "The days of patching up legacy systems are gone; companies are looking to invest in new systems that will protect against cybersecurity threats from a proactive risk mitigation perspective."

Getting ahead of cyberthreats requires conducting more regular cybersecurity risk assessments, honing a robust regulatory compliance strategy, and updating processes and procedures as needed, she says.

Health care

Earlier this year, Change Healthcare, among the world's largest health care clearinghouses for medical claims, experienced a **devastating cybersecurity incident**. The event shut down the organization's electronic payment platforms and pharmacy network services. The impact continues to be far-reaching for any health care system that relied on Change Healthcare's services. Critical processes at health care organizations came to a halt, hampering both providers and patients.

According to an **American Hospital Association** survey, 94% of hospitals are experiencing a financial impact from the Change Healthcare cyberattack, with more than half describing it as "significant or serious."

"Many medical practices and health systems continue to experience major revenue struggles that threaten their overall financial viability not only due to the revenue cycle disruption, but also because of the impact on basic financial operations such as processing payroll," says Greg Vetter, an RSM principal and health care cyber risk services leader.

Operational and communications challenges are many when a breach involves sensitive patient information, he says. Vetter recommends organizations shore up their cyber flanks and consider the following:

Conduct a robust review of business continuity and disaster recovery planning. This work enables an organization to sustain essential operations during a major disruption to systems, processes, facilities and more. An organizational business impact analysis, often the foundation of recovery planning, should include essential vendors and other third parties supporting critical business activities—a measure that would have helped organizations identify the Change Healthcare risk and provided the opportunity to respond more effectively.

Take inventory of all third parties deemed critical to the organization. The process for identifying high-risk vendors is nuanced and must be thoughtfully executed, as risk is not just driven by vendor spend or proximity to the largest applications or processes. The inventory should document the services provided and business processes the vendor supports, as well as the type of data stored, processed or transmitted on the organization's behalf. In addition, organizations should consider their extended vendor ecosystems that include fourth parties, along with the vendors and service providers third parties rely on. Due diligence should be conducted regularly during the vendor relationship.

Carefully evaluate the overall cyber program. Cyber incidents can originate with a vendor and other third parties, but the greatest risk to an organization remains the failure of their internal cyber protections. Organizations should regularly assess their program to ensure it is meeting the requirements of a rapidly changing digital world.

Manufacturing

For those who work on or near a factory floor, safety protocols have long been a critical priority; appropriate eyewear and steel toe boots are often essential protection around machinery and production lines.

But manufacturing safety has evolved well beyond the physical. As manufacturers become more interconnected—combining traditional IT functions, Internet of Things devices and operational technology on the factory floor—strong cybersecurity measures and thorough risk management are paramount. Further, companies can learn lessons and draw parallels between physical safety and cybersecurity for personnel who have long understood the value of safety but don't yet see the value of cybersecurity.

"For industrial companies, cybersecurity is the new safety," says David Carter, an RSM industrials senior analyst. "And as more companies move their data centers into the cloud, it's changing the way they operate."

Companies need to think holistically about cyber risks to build cyber resilience. That means integrating cybersecurity risk management into the broader scope of enterprise risk management, rather than allowing it to exist in its own silo.

"Some manufacturing leaders might be of the mindset that because manufacturers don't handle large quantities of personally identifiable information—the way health care or consumer products companies do, for instance—they are at lower risk for a cyberattack," says Carter. "On the contrary; manufacturing is often among the most vulnerable sectors when it comes to cybersecurity breaches."

For industrial companies, weak cybersecurity endangers not just computer programs but also factory systems and power plants. Furthermore, the outdated infrastructure of many manufacturers makes them a target, and cyberattacks on operational technology might hinder production, order fulfillment and, ultimately, profitability.

Businesses should tailor their cybersecurity controls and protections based on the risks they face. A few areas for manufacturers to prioritize include identity access management, cloud security processes, zero-trust architecture and penetration testing.

Professional services

Cybercriminals balance their desire for big paydays with the odds of success. Many large law firms, consultancies and ad agencies tend to have strong cybersecurity, so hackers often target the smaller professional services firms they perceive as more vulnerable.

While firms of all sizes are taking cybersecurity seriously, their drive to protect digital assets does not always line up with their resources, says Michael Gerlach, an RSM partner and professional services senior analyst.

"The bigger firms have policies, testing, training, cyber insurance and tools that you would expect," Gerlach says. "But as you move farther downstream, it gets a little less refined. Smaller firms typically have less of a cyber strategy."

Because of limited resources, those firms often make do with what they have, he says, adding that he has observed a "hodgepodge approach" that frequently relies on a mix of third-party providers.

Regardless of an organization's size, leaders need to understand how their data is stored and identify weak spots in their systems, says Gerlach, who advocates a holistic approach to cybersecurity that takes into account all of an organization's systems. That can be a tough transition for professional services firms, which often have decentralized leadership and disparate workstreams.

"Some firms say, 'Let's go down the AI path' or 'Let's go down the cloud path,' and that's good," Gerlach says. "But with each investment in technology, you also have additional risks and exposure that you need to address. It's a matter of ensuring that professional services firms are being diligent about the changes in cyberthreats and working to mitigate them."

Real estate and construction

The cybersecurity threat facing real estate and construction companies may be overshadowed by publicity around prominent attacks in other industries, but these sectors are equally at risk.

An intricate network of players, combined with the mobile nature of work in this vast ecosystem, make real estate and construction prime targets for cybercrime. The high volume of field-to-office communication and payment transactions creates a playground for criminals to unleash social engineering, phishing attacks and other scams to exploit people and steal information and money.

"While cyber liability insurance helps protect companies against financial loss in the event of an attack, education and cybersecurity measures should be the first line of defense," says Chris Wetmore, an RSM principal and leader in the firm's technology advisory practice. Construction workers and others in these fields often connect to open networks, unaware that they are putting critical information at risk, he says.

Employee awareness training represents the bare minimum for effective cybersecurity governance. Companies doing business in multiple states must also adhere to nationwide data privacy and protection laws. For government work, such as Department of Defense contracts, compliance with the Cybersecurity Maturity Model Certification (CMMC) 2.0 program **is now a requirement**. Meanwhile, real estate investors increasingly want to see controls in place to protect their financial information.

Many real estate and construction companies are challenged by inadequate resources for training, technical support and internal controls, which has led to more outsourcing.

"We are seeing more companies leveraging cloud services and other technologies to mitigate cybersecurity risk, and also engaging third-party firms to manage their technology stack," says Matt Riccio, an RSM senior analyst for the real estate industry.

Riccio notes that ransomware, fraudulent wire transfers and data theft are commonplace among middle market real estate and construction firms. Finding protection against these cyberthreats is increasingly important as attacker tools and strategies grow more sophisticated by the day.

On the plus side, emerging cybersecurity technologies enhanced by cloud computing, artificial intelligence and machine learning are continually advancing to help organizations stay one step ahead of cybercriminals.

Retail

E-commerce sales rose 7.6% last year, according to the U.S. Census Bureau. By all accounts, online retail shopping will continue to increase—and along with it will come increased opportunities for cyberattacks.

Cracking of consumer passwords and the creation of ghost websites are among the leading threats to retailers, making identity management a priority, says Nick Stuart, an RSM senior analyst for the consumer products industry. Ghost websites are replicated websites that look exactly like a retailer's website, but with a fake URL. When the consumer checks out on a ghost website, the criminals will steal personal information, including credit card details. Sound security strategy includes authentication and other access protocols to combat these threats.

"Given various online platforms, passwords are prevalent, from consumer loyalty accounts to store apps and checkout systems," he says. "Once breached, personal data, shopping history, financial information, credit card numbers and more are grabbed for criminal use."

While security is paramount, retailers also want to limit "friction," the frustration their customers experience when online purchases require additional effort and time. Consumers want less hassle with fewer clicks to check out, even as they expect the process to be secure, Stuart says.

Technology can help with this balancing act. Authentication apps such as Shopify's Shop Pay and Amazon Pay, as well as payment platforms like Apple Pay can amp up security while reducing checkout time. They securely store consumer information so that shoppers avoid reentering data such as shipping information every time they make a new purchase. These platforms rely on biometric passkeys, PINs and other techniques in lieu of two-factor authentication and passwords—tactics that customers often find frustrating.

"The process allows speedy checkout and a satisfied customer, one that will hopefully be back for future purchases," Stuart says.

Fortifying identity management also calls for a comprehensive data governance program, cloud migration and constant monitoring of relevant privacy and security regulations. These measures will help protect customer data, maintain business continuity and build trust with consumers, Stuart says.

Technology

The technology industry faces a host of challenges to protect its complex systems, data and users amid pervasive cyberthreats.

For midsize technology companies, in particular, the basics are often a good place to start, says Kurt Shenk, an RSM partner and senior technology industry analyst. These predominantly private businesses, which often grow quickly due to organic growth, infusions of private capital, or acquisitions, are focused on scaling up, so they can have a blind spot for their cyber vulnerabilities, he says.

"Some of the things that might be second nature at a large firm are not necessarily in place at midmarket tech companies," says Shenk, noting a lack of incidence response protocols, education around threats such as email phishing or a clear understanding of cybersecurity insurance coverage. "What's the procedure, who is getting involved and how do you respond when something takes place?"

Even the best preparation cannot always thwart sophisticated attacks, says Shenk, who notes that several of his technology clients now find it necessary to keep bitcoin on their books in the event they fall victim to a ransomware attack and must pay bad actors to release their information.

Well-known technology corporations have been among the most widely reported breaches in recent years. As of late 2023, the SEC began requiring public companies to report "material" cybersecurity incidents within four business days and to disclose annually how they manage cybersecurity—both measures designed to protect investors.

Meanwhile, the use of AI presents technology firms with great opportunity for innovation but also brings additional cyber risk, Shenk says. The European Union in March gave final approval to a set of protections around AI use intended to take effect in about two years, including prohibiting AI-powered social scoring systems and biometric tools that attempt to surmise an individual's race, politics or sexuality. The United States, by contrast, has yet to put forth similar restrictions.

But Shenk believes the recent SEC requirements may portend a period of heightened regulation that could govern private companies as well.

"The beginning of regulation is there, and it seems like something that will continue," he says. "Companies are focused on it."

Telecommunications

The cybersecurity concerns of telecommunications companies continue to increase and diversify as more people, institutions and devices rely on telecom networks. Bad actors are homing in on their targets accordingly, and strengthening their capabilities by putting technological advances to nefarious use.

For telecom companies, this evolution underscores the importance of secure infrastructure, stringent protocols and dedicated vulnerability testing, says Andrew Fedele, a telecommunications senior analyst at RSM.

"With each node you add to a network, the more entry points you have for bad actors," Fedele says. "Everything that's tech-enabled can be an entry point. Layer the capabilities of artificial intelligence on top of the increased access points, and suddenly bad actors are able to proliferate more quickly or use large language models to penetrate systems quicker. It's really concerning."

Just as cybercriminals' motivations may vary, so do their methods, which complicates prevention for telecom companies whose networks or infrastructure may be targeted. Whether a nation-state illegally accesses another government's information via a network connection, or an individual doxes a corporate executive through a phishing scheme, telecom companies can be proactive by taking note.

"It's being ready, testing vulnerabilities, making sure they have a plan and getting ahead of the curve," Fedele says. "In recent attacks, what are the weaknesses? How have cybercriminals been accessing a sensitive environment? How do we address those entrance points on our end?"

Meanwhile, regulatory developments are creating additional layers of considerations and potential challenges for telecom companies.

The U.S. Federal Communications Commission in March 2024 approved the creation of a voluntary labeling program for smart devices that meet cybersecurity criteria developed by the National Institute of Standards and Technology. One of the program's objectives is to encourage manufacturers to develop internet-enabled products with security-by-design principles in mind.

Additionally, the Cybersecurity & Infrastructure Security Agency in March 2024 proposed reporting requirements under the Cyber Incident Reporting for Critical Infrastructure Act. Organizations across critical infrastructure sectors, including communications, would be required to report cyber incidents within days. Not only could these requirements improve response times and awareness in matters of national security, they are a big win for consumers, who often learn about breaches of their data many months after the fact.

Telecom companies will need to monitor how reporting requirements evolve and think strategically about compliance processes. This only adds complexity to cybersecurity challenges, as companies try to keep pace with bad actors and advancing technologies.

The takeaway

Cybersecurity attacks are elevated and potential threats loom, leaving middle market companies at substantial risk. Many companies have become complacent about cybersecurity amid fatigue after consistently hearing about risks and attacks for several years. But hackers are persistent and will take advantage of any vulnerabilities or control gaps in an organization's defenses.

Middle market companies need to evaluate their strategies to resist and respond to attacks and take advantage of opportunities to strengthen their cybersecurity strategy. Potential adjustments include optimizing existing security tools, implementing modern identity access plans and leveraging managed security services to augment internal IT personnel who often can't keep up with evolving cybersecurity concerns and regulatory demands.

The cybersecurity landscape is complex, and addressing challenges certainly is not easy. But companies must remain vigilant to protect sensitive data and ensure sustainable operations.

Methodology

The RSM US Middle Market Business Index survey data in the first quarter of 2024 was gleaned from a panel of 1,500 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 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 2024 first-quarter survey was conducted from Jan. 8 to Feb. 16, 2024. Information was collected by phone and online survey from 403 executives, including 163 panel members and a sample of 240 online respondents. Data is weighted by industry.

U.S. Chamber of Commerce

A review of the current administration's cybersecurity priorities

President Joe Biden assumed office in January 2021 amid an unquestionably challenging environment for cyberthreats. A month earlier, a cybersecurity researcher from Google subsidiary Mandiant discovered an exploited vulnerability in network management software developed by SolarWinds. Over the next several weeks, a series of high-profile ransomware attacks breached a range of companies, including natural gas provider Colonial Pipeline, meatpacker JBS Foods and IT software maker Kaseya. Meanwhile, the world was confronting the scale of the intrusion, as the blame fell on Russian threat actors. The events colored the new administration's priorities and programs of work, which the U.S. Chamber of Commerce has organized into three categories.

Priority 1: Raising baseline cybersecurity requirements for critical infrastructure

From the first **security directives** issued by the Transportation Security Administration to the "More Than a Password" **information campaign** developed by CISA (Cybersecurity & Infrastructure Security Agency) to **open letters to the business community**, the administration's first cybersecurity priority was to voluntarily leverage regulations to raise baseline requirements protecting critical infrastructure.

Why this matters: The Biden administration expects organizations of all sizes to increase their cybersecurity and risk **management investments.**

Applicability: The administration has taken a sector-by-sector approach to review each of the 16 infrastructure sectors designated vital to the United States under the USA Patriot Act, the Homeland Security Act of 2002, and Presidential Policy Directive 21—all measures enacted to bolster security for the country's physical and digital infrastructure.

What does good look like? Standards-based compliance is increasing the minimum expectation by governments. The U.S. Chamber recommends that organizations use the Cybersecurity Framework developed by NIST (National Institute of Standards and Technology) to guide risk management and to conform with ISO/IEC 2700X, which was developed jointly by the International Organization for Standardization and the International Electrotechnical Commission, as well as NIST's SP 800-53 and 800-171 standards.

Priority 2: Securing the software supply chain and driving security by design

Second only to legitimate credentialed access, supply chain threats and attacks are among organizations' top cybersecurity risks.

Administration action: The Biden administration published the definitive policy directive for software supply chain security, **Executive Order 14028, Improving the Nation's Cybersecurity**, in May 2021.

Why it matters: EO 14028 sets forth roughly 60 action items related to supply chain security, including these minimum elements: a software bill of materials, guidelines for software supply chains and updates to regulations for contractors.

Applicability: Acting through the Federal Acquisition Regulatory (FAR) Council, the Biden administration will require new software security and incident reporting by nearly all federal contractors.

Priority 3: Enhancing the government's visibility of cybersecurity incidents

The **United States**, the **European Union** and other governments around the world have promoted initiatives to close the visibility gap between government agencies and cyberattack victims. The U.S. Chamber has also promoted **global principles** to guide policymakers who are considering the establishment of business incident reporting requirements.

Why does disclosure matter? The first of two theories contends that public disclosure of material cyber incidents will prompt prioritization and longer-term investment by organizations at the executive level. The second theory purports that government agencies are blind to the heightened threat environment, and only enhanced visibility will ensure that they: 1) better understand national risk, 2) prioritize resources for the most at-risk entities, and 3) tailor improved mitigation for victims.

Cost versus cyber risk reduction? CISA recently estimated that implementing its CIRCIA (Cyber Incident Reporting for Critical Infrastructure Act) rules will cost CISA and the industry $2.6 billion over 11 years of implementation. Will the tidal wave of incident reports actually result in risk reduction? Despite policymakers' best intentions, probably not—at least in the near term. However, there may be incremental reductions in cyber incidents and breaches on a yearly basis.

For more information, contact Vince Voci (**vvoci@uschamber.com**), vice president for cyber policy and operations at the U.S. Chamber of Commerce.

The ongoing evolution of identity and access management

As digital identity becomes more important, companies must focus on strategy

Cybersecurity remains a chief concern for middle market companies, and the battle against cybercriminals shows no signs of slowing. Hackers will take advantage of any vulnerability they can find to breach a network, and history has shown that accounts and systems secured by passwords are inherently at risk. Instead, proactive companies are focusing on passwordless digital identity strategies, with identity and access management (IAM) strategies at the forefront of that movement.

Many security strategies that companies commonly employ can lead directly to cybersecurity concerns. In the 2024 RSM US MMBI Cybersecurity Special Report, the leading digital identity measures among middle market companies were providing access as needed (31%), single identity access to systems such as single sign-on (24%), and disparate usernames and passwords (22%).

No method is perfect, but the first two of these strategies often require security personnel to manually commission and decommission access, which can be a challenge when companies have few internal resources and additional qualified talent can be difficult to hire and retain. Further, utilizing disparate passwords is no longer a truly effective strategy, as hackers can often guess passwords or user may write complex logins down on paper or store them in a file on their computer, creating low-hanging fruit for potential criminals.

The potential answer lies in the fourth most popular answer in the MMBI survey: Passwords are a thing of the past. While only 11% MMBI survey respondents indicated that they have gone passwordless at this point, the momentum behind these IAM strategies is growing. And for good reason.

In today's technology environment, users, systems and devices all have their own identities, and often multiple identities, depending on what they are trying to accomplish. Unfortunately, those are difficult to harness and manage within traditional digital identity strategies.

"There are a couple of different aspects to IAM, and every company comes at it in different ways," says Chad Wolcott, a managing director at RSM. "Ultimately, I see more organizations looking at IAM as an enabler to confidently manage those digital identities. It allows companies to manage that entry point into the organization and do it in an efficient and secure way."

IAM enables companies to manage some very tactical security areas more effectively. For example, an effective IAM approach can help onboard people quickly so they can be productive immediately and access can be removed with they leave the organization. There are other security controls that can do that, but IAM creates a frictionless experience for employees and customers.

IAM is all about creating better user experiences within a company's overall cybersecurity framework. From a security and access perspective, it's the best of both worlds.

"It uses identity to help deliver an experience that empowers the user—whether that's a customer or a member of your workforce," says Daniel Gabriel, an RSM principal. "It's really more of a business tool than anything else anymore."

As companies consolidate and perform transactions, IAM can be a valuable tool to maintain security and create a consistent user experience.

"As companies buy up their competitors, you can have the same population that has different views of the organization," says Wolcott. "If I have accounts with five different small banks and they all get acquired by a regional bank, that bank sees me as five different people. That's not the experience I want as a customer. Using IAM to merge all that information together into a single experience is hugely powerful because then you can apply other controls on top of that to ensure everything is happening securely."

Establishing an IAM approach is not a technology-first problem. Companies need to understand the key drivers in the organization and determine a strategy around what they want to accomplish. Use cases that need to be factored in should be detailed and then rightsized to fit the program before execution.

"Thirty percent of the identity challenge is technology," says Wolcott. "The other 70% is the people, the process and dealing with bureaucracy. So, the best way to start is to understand what the organization's needs are, and then build up that road map to meet those needs over time. It's about incremental progress over delayed perfection. Do not try and do everything out of the gate—start small and build from there."

Emerging tech and talent challenges highlight need for managed security services

As digital identity becomes more important, companies must focus on strategy

Creating an effective cybersecurity approach is not optional for middle market companies, as suffering a cyberattack can have a harmful ripple effect across the business. But small internal security groups can feel overwhelmed and outnumbered as they contend daily with criminals from countries around the world. Managed security services solutions have become a critical strategy for middle market companies to augment existing personnel or take over entire functions, establishing a security strategy that can stand up to modern threats.

In the 2024 RSM US Middle Market Business Index Cybersecurity Special Report, 61% of respondents indicated they had two or fewer data security and privacy employees. With companies becoming more digital every day and the potential attack surface expanding, companies often don't have enough internal resources to cover evolving risks.

In addition, with the continuing challenges in the labor market, qualified security talent can be difficult to hire and retain. And the internal personnel companies do have may not have the right skills to keep up with the rapidly evolving threat environment. Simply stated, companies often need help.

"Operations that require a large investment in technology are typically where it is tough to get people that have the necessary skill level," says Daniel Gabriel, a principal at RSM. "So, companies turn those functions over to an experienced third-party provider. It is often a reaction to the inability to get the right talent in the organization, but it's a good way to augment a team."

Managed services have been a trusted strategy for middle market companies within several functions for many years. But in recent years, the strategy has expanded to encompass security and privacy services, giving companies options when internal resources are not sufficient.

In addition, while managed security options were initially limited to monitoring services, several other services are emerging to meet the specific needs of the market. For example, RSM Defense is RSM's managed security monitoring solution, but also available are new services for governance, risk and compliance as well as a loan staff strategy that can provide experienced staff for as long as a company needs them.

"I am seeing more companies that want a provider that can provide multiple services, says Gabriel. "They don't want to work with 30 service providers. Instead, they want a provider who can provide multiple things and package those up for seamless interaction."

In recent years, how companies engage with managed services providers has changed. Previously, such providers were treated as third parties that provided little value—they just handled a process nobody wanted to do. But organizations were not typically getting the results they anticipated, and they began looking for more value from providers.

"Now, when companies engage us in conversations about managed services, it's about what outcomes they will receive," says Gabriel. "It's not only about how we will support a product or tools, but also about what value the company will gain by entering a managed services agreement."

The way the market is buying managed services is pivoting, and companies are getting better at determining what they want.

"Companies have become more sophisticated, and they are looking for more things as a service," says Gabriel. "That's where they can offload repetitive tasks or things that they do not have the personnel or experience to handle themselves and get results."

A managed security services strategy provides several direct benefits, including scalable solutions that can grow with demand and advanced tools that companies may not have access to otherwise. In addition, with the modular approach and the growing depth of managed security solutions, companies have seamless access to whatever resources they need to secure their environment.

As companies implement more technology and cybersecurity risks become more complex, managed security services become a more attractive option. These services are rapidly moving toward becoming a core component of middle market security strategies, providing deep experience, more effective protection and enhanced flexibility at a predictable cost.

Successfully managing artificial intelligence security and privacy risks

Many companies remain concerned about risks as AI usage increases

Artificial intelligence (AI) is a hot topic in all segments of the economy, as companies evaluate how they can take advantage of potential increases in efficiency and productivity and make more rapid, informed decisions. Even so, organizations cannot lose sight of the potential risks related to AI.

Not surprisingly, AI use is rapidly expanding in the middle market as more solutions become accessible and companies discover new use cases. In an upcoming RSM US LLP report that details AI use in the middle market, more than three-quarters of survey respondents (78%) say their organizations use AI, either formally or informally, in their business practices. Seventy-seven percent report using generative AI.

Generative AI is gaining significant momentum within midsize companies, as 74% of middle market executives report having a dedicated generative AI budget and 85% say that the technology has had more of a positive influence on their organization than expected.

Despite that positive impact, companies understand the potential risks of the emerging technology. Survey data suggests that some companies that have adopted generative AI have data security and privacy concerns about the technology. In addition, for those not currently planning on using generative AI, 46% cite data security and privacy as the leading reason.

Many of the perceived risks when implementing generative AI are rooted in common misconceptions about the technology. First, many feel like every piece of data sent to a large language model can be viewed by another party and lead to a vulnerability or exposure.

RSM Director Dave Mahoney detailed some potential scenarios. "If a user uploads a document to a public, large language model chatbot like ChatGPT, Gemini or other popular options, then yes, the company has lost control of that document and it is subject to the AI provider's privacy conditions," he says.

"The same scenario can occur with prompts," he continues. "If someone takes a spreadsheet that has sensitive information in it and sends it within a prompt, that data could be at risk."

If information is meant to be kept private, companies can use application programming interfaces (APIs) that do not use data to train models. But if a user shares sensitive data in an open-source application, the company gives up control.

Essentially, companies need to have effective controls over sensitive information to ensure that it is not shared with people that should not have access to it. But this is not a new concept—it is just a new application.

"So, it's not just a simple 'Hey, if you use AI, your data is being stolen,'" says Mahoney. "It's the same as a user emailing sensitive data outside of the organization or accidentally sharing it with a client that shouldn't have access. That's not an AI problem. That's a data loss problem that already existed."

In addition to those risks, AI tools and applications can present other unique threats. For example, if a middle market company wants to build a fully enabled large language model that requires expert-level information and feedback, it will likely be derived from a similar model someone else has built.

Whether the model is hosted by a provider or built internally, it is subject to access risks. Companies don't want information to be exposed, especially if they operate in a field that routinely handles sensitive data, such as the financial, legal or health care sectors.

However, practices and techniques to safely build and maintain models are available. Companies must think about where the model lives, what information the model can have access to, and whether anything happened in the development or the operation of that model that could inject additional risk. If the company does not control and own the model, then a provider could increase the level of risk.

"I do agree that is a concern," says Mahoney. "But that just requires doing your homework and having an understanding of how the technology works, what you're buying and how it operates at a fundamental level."

In these scenarios, the risks are manageable and largely related to internal controls and education. Regardless, these challenges should not be barriers to evaluating and implementing generative AI solutions. Apprehension about new technology is normal, but companies cannot hesitate for too long.

"In my opinion, if you plan to be an effective leader in almost any business, you have to get your hands around AI and figure out how you can start leveraging it to drive efficiency and scale operations," says Mahoney. "Otherwise, you will be left behind, both professionally and in terms of the resiliency of your business."

Ongoing SEC cybersecurity requirements

The U.S. Securities and Exchange Commission in July 2023 released final cybersecurity rules requiring public companies to disclose details on material incidents as well as information on cybersecurity risk management, strategy and governance.

The SEC's move to extend its cybersecurity requirements signifies a pivotal evolution in the regulatory landscape. It demands proactive measures, strategic planning, a holistic approach to safeguarding data and operations, and a shift from an approach emphasizing regulatory environments versus the broader enterprise. The SEC cybersecurity rules require a closer focus on three areas: oversight of cyber risks, cyber risk management, and disclosure of material incidents and risks.

While many larger public organizations likely already have processes and resources in place to meet these requirements, emerging and middle market public companies may need to make structural and cultural changes to enhance or adopt cybersecurity oversight, management and reporting processes to comply with the final rules.

The rules require the disclosure of cybersecurity incidents on Form 8-K (Form 6-K for foreign private issuers) within four business days if deemed material. Registrants must describe the material aspects of the incident's nature, scope and timing, as well as its material impact or reasonably likely material impact on the registrant in the newly introduced Item 1.05 of Form 8-K. Delayed filing is allowed if the U.S. attorney general determines that immediate disclosure would pose a substantial risk to national security or public safety.

In addition to completing Form 8-K, registrants must file Form 10-K to describe their cybersecurity risk management and strategy, management's role in assessing and managing material risks from cybersecurity threats, and their board of directors' oversight of cybersecurity risks.

The SEC rules define three key terms as follows:

- **Cybersecurity incident:** An unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity or availability **of a registrant's information systems or any information residing therein.**
- **Cybersecurity threat:** Any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity or availability of a registrant's information systems or any information residing therein.
- **Information systems:** Electronic information resources owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of the registrant's information to maintain or support the registrant's operations.

To properly assess the aggregation of related immaterial incidents, registrants must continually refine their incident response management process. This includes maintaining a robust incident logging process to record incident details. Ongoing evaluation of materiality arising from the aggregation of these incidents is imperative to enable informed disclosure decisions.

In light of the SEC's broadened cybersecurity requirements, organizations must adopt a proactive stance to achieve compliance and enhance their overall security posture. Consider the **following crucial steps** to guide you on this journey:

- Conduct comprehensive asset inventory and management.
- Implement a unified control framework.
- Balance compliance and protection.
- Implement continuous control assessment and monitoring.

In addition to the SEC issuing new rules, the U.S. Federal Trade Commission amended its Standards for Safeguarding Customer Information to require all nonbanking financial institutions to report a data breach incident within 30 days after discovery if it involves the information of at least 500 consumers. That **Safeguards Rule update** will go into effect in May 2024.

Aggregated from:

https://rsmus.com/insights/services/risk-fraud-cybersecurity/understanding-and-addressing-new-sec-cybersecurity-rules.html

https://rsmus.com/insights/services/risk-fraud-cybersecurity/sec-expectation-materiality-assessment-cybersecurity-disclosures.html

https://rsmus.com/insights/services/risk-fraud-cybersecurity/going-beyond-compliance-to-strengthen-your-organizations-security.html

https://rsmus.com/insights/services/risk-fraud-cybersecurity/navigating-sec-cybersecurity-requirements.html

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