

RSM US MIDDLE MARKET BUSINESS INDEX CYBERSECURITY

SPECIAL REPORT

2022



U.S. Chamber of Commerce



TABLE OF CONTENTS

- EXECUTIVE SUMMARY 3
- HOW THE CYBERSECURITY OUTLOOK IS RAPIDLY EVOLVING IN THE MIDDLE MARKET 6
- A COMPARISON OF U.S. AND UK CYBERSECURITY RISK PERSPECTIVES 8
- INFORMATION AND DATA SECURITY 10
- CYBER INSURANCE 13
- RANSOMWARE ATTACKS 16
- BUSINESS TAKEOVER THREATS 18
- PRIVACY PROTECTIONS COMPLIANCE 20
- MIGRATION TO THE CLOUD TO ENSURE DATA SECURITY 22
- METHODOLOGY 23
- ADDITIONAL REPORTING REQUIREMENTS PLANNED FOR CRITICAL SECTORS AND PUBLIC COMPANIES 24
- MANAGING CYBERSECURITY THREATS RELATED TO GLOBAL CONFLICT 25
- UNDERSTANDING CYBERSECURITY RISKS RELATED TO DIGITAL TRANSFORMATION 26
- MIDDLE MARKET LEADERS DETAIL SUPPLY CHAIN CYBERSECURITY CONCERNS 27



EXECUTIVE SUMMARY

Moving in the **right direction**

Reported breaches drop, but significant cybersecurity concerns persist

In recent years, cybersecurity has been a considerable concern for middle market companies, although the specific threats are constantly in flux. Last year was no different, as organizations encountered a roller coaster of risks, from lingering threats related to the COVID-19 pandemic to geopolitical conflicts and economic uncertainty underscored by the war in Ukraine. As is often the case, bad actors in cyberspace could come from a variety of angles on any given day.

Yet again, breaches at large entities grabbed the majority of the headlines over the past year. Those incidents continue to prove that no organization is truly immune to a breach, even larger enterprises that inherently have more resources to implement advanced controls and are generally now doing a better job in fortifying their environments. The middle market, often escaping public attention, has become even more of a focus for criminals as they push downward to find vulnerabilities at smaller companies with less mature controls.

However, there is good news. The number of breaches reported among middle market companies is slightly

dropping as protections become more available and executives understand the consequences related to potential incidents. But even with enhanced protections in place, companies cannot afford to let their guard down. It's a constant battle against those who seek to access files, systems or funds illicitly—being reactive instead of proactive is no longer an option.

Middle market leaders provided insight into the evolution of their cybersecurity approaches in a 2022 first quarter RSM US Middle Market Business Index survey. The survey polled 402 senior executives at middle market companies about their cybersecurity and data privacy challenges, detailing the frequency and severity of

22%  ERROR

of middle market executives claimed their company experienced a data breach in the last year

REPUTATIONAL RISK



"I don't fear the loss of data. I'm very confident that maybe we might at most lose 24 or 48 hours' worth of data. I fear the PR aspect of it of having to send that required communication to anybody who might be affected. You don't want to go to your members and say your data was compromised. They think less of you."

NONPROFIT EXECUTIVE

attacks, and ongoing concerns, while providing a glimpse into how the largest segment of the U.S. economy is implementing controls and strategies to address security threats and fight back against cybercriminals. In many cases, survey 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, 22% of middle market executives claimed that their company experienced a data breach in the last year, representing a sizable drop from 28% in last year's survey. Larger middle market organizations were most at risk once again (30%) compared to smaller counterparts (12%), but both showed a decrease in attacks.

Even with the decline in reported attacks, companies recognize the risks posed by the current dynamic threat environment, with 72% of executives anticipating that unauthorized users will attempt to access data or systems in 2022, a sharp rise from 64% last year and the highest number since RSM began tracking data in 2015. In response, more middle market companies are embracing a managed services approach with third-party providers. This response is demonstrated in the survey, as 60% of respondents disclosed that they have an internal, dedicated data security and privacy function, a drop from 71% last year.

In addition, cyber insurance continues to be a key element of cybersecurity strategies for the majority of middle market executives. The RSM survey found that 61% of companies carry such a policy, a slight drop from last year's 65%. The data shows that the number of smaller middle market companies utilizing cyber insurance has slightly increased, while their larger counterparts reported a significant drop in coverage.

The data privacy landscape continues to evolve in the United States with constant dialogue about who should collect and possess sensitive data, and how it should be stored. The discussion is no longer just about how information is secured but why organizations need that

THE DREADED CALL



"I dread the call, of course, from our current provider that, well, something happened. Something happened last night and we couldn't repel it. And nobody can get into their system this morning. I hope that call never comes. We've had several calls informing us that, you know, the bad actors are still out there trying."

PETROLEUM COMPANY EXECUTIVE

data in the first place. The European Union's General Data Protection Regulation, known as GDPR, was a trailblazing piece of legislation that went into effect in 2018 and has served as a blueprint for data privacy standards worldwide.

For example, the GDPR has inspired data privacy regulations in several individual U.S. states, including the well-known California Consumer Privacy Act. At least 15 other states have some level of data privacy standard, and because of bipartisan support, federal guidelines are likely at some point.



“We see businesses of all sizes encountering cyberthreats, such as ransomware attacks. With the ongoing Russia-Ukraine conflict, the U.S. homeland and national security communities are urging businesses to take steps to protect their networks and partner with the government. The Chamber will continue to advocate for the importance of public-private partnerships, operational collaboration, and information sharing to increase our nation's cybersecurity.”

Matthew Eggers

Vice President of Cyber Security Policy,
U.S. Chamber of Commerce



A MOVING TARGET

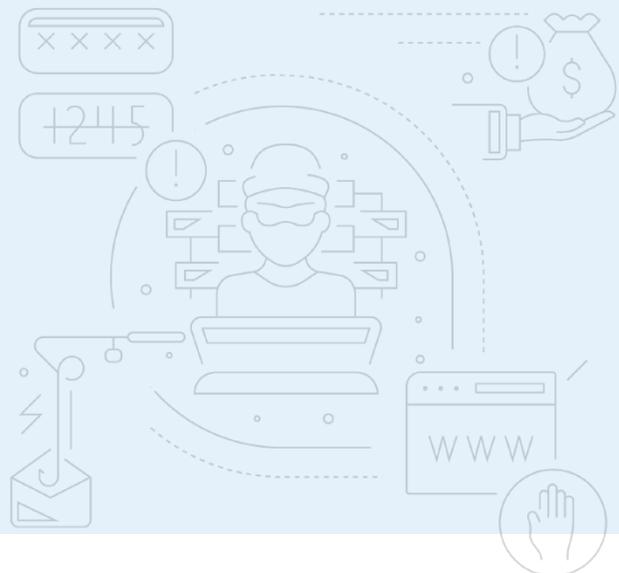


“Cybersecurity is this continually moving target that you have to be on top of all the time. It’s a huge risk to the business, and it’s not something that you can put on the back burner and just say it’s going to be OK.”

MANUFACTURING EXECUTIVE

As companies contend with more data privacy regulations as time goes by, awareness will be critical to avoid potential penalties. With that in mind, RSM MMBI data shows that 58% of middle market executives are familiar with the requirements of the GDPR, a slight increase from 2021. In addition, 96% of executives report that preparing for emerging privacy legislation or regulations is at least a priority of minor importance, similar to last year’s findings.

Middle market companies face an increasingly volatile cybersecurity environment, with threats coming from more directions than ever before and more skilled criminals targeting the segment. To help ensure effective strategies and controls are in place, companies must take advantage of benchmarking opportunities and learn from the experiences of their peers. 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.





How the cybersecurity outlook is rapidly evolving in the middle market

Tech advances are overshadowed by expenses and geopolitical concerns

In recent years, cybersecurity has steadily risen among the list of concerns for middle market companies, with emerging threats dictating frequent changes in risk management approaches. However, in addition to managing evolving external threats, several operational challenges are now taking center stage in developing an effective cybersecurity strategy.

The costs related to cybersecurity are fluctuating across organizations; expenses are actually going down in some areas, while in others, they have become exponentially higher. From a technology standpoint, more companies are moving data and applications to the cloud for access to a higher level of protection and controls, with many infrastructure costs going away.

However, as companies in all sectors are finding, the talent to manage that cloud environment is becoming more expensive and more difficult to find and retain.

From a talent availability standpoint, many candidates are not entering the workforce with the necessary knowledge to manage cloud technologies. In many cases, colleges and universities simply aren't preparing students with the necessary cybersecurity skill sets. And unfortunately, after people are trained in a corporate environment, they will likely have opportunities to leave for higher-paying positions. Companies will need more qualified resources as time goes by, but finding and retaining that talent is a repeating and increasingly expensive cycle.





“The talent level is not catching up as fast as it needs to. As a country, we are not producing the number of people with the necessary cybersecurity skills that companies critically need.”

Tauseef Ghazi

National leader of security and privacy services
RSM US LLP



“The talent level is not catching up as fast as it needs to,” said Tauseef Ghazi, RSM national leader of security and privacy services. “As a country, we are not producing the number of people with the necessary cybersecurity skills that companies critically need.”

Ken Stasiak, RSM national leader of cyber testing and response, further emphasized the cybersecurity talent concerns many organizations face. “I think it’s more of a skill set gap,” he said. “While universities are training new hires to perform the basics, companies need more advanced and expert knowledge.”

The cost of cybersecurity labor and the talent gap are not necessarily new issues in the middle market, but options to alleviate those concerns are becoming exhausted. For example, many companies have offshored technology resources to countries such as India in the past. However, the demand for talent has driven wages up, so that strategy may no longer be advantageous from a cost perspective.

“The Indian technology skills market has gotten severely saturated over the last few years,” said Ghazi. “Right now, resource costs in India are rising just the same as they are for onshore resources. The sudden shift in demand during the pandemic with many companies moving systems and applications to cloud platforms and switching to a managed services model for information technology infrastructure has holistically increased the demand on outsourcing.”

While cyber insurance is a key element of the cybersecurity arsenal for many middle market companies, premiums are also escalating. For companies

that can procure coverage that fits their needs, there is now more emphasis on demonstrating that the right controls and protections are in place if an incident occurs. Without that proof, a claim can be denied with potentially very harmful results.

These costs will remain a big issue for the middle market for the foreseeable future. Finding the right employees and retaining them as long as reasonably possible or working with a qualified third party that aligns with your culture and goals will be of paramount importance for protecting your organization from cyberthreats moving forward.

In addition to cost and staffing challenges, the Russia-Ukraine conflict has increased the importance of taking a proactive cybersecurity approach and ensuring the strength of controls. Hacktivists (someone who launches cybersecurity attacks in support of a political cause) have emerged who are sympathetic to both Ukraine and Russia. And President Biden has made recent statements warning of potential Russian cyberattacks on commercial entities and potentially on critical infrastructure.

Cybersecurity threats inherently move quickly. And while many of the costs related to cybersecurity have gone up, middle market companies do not have a choice when it comes to securing their systems and data. They do, however, have options. Being proactive in taking advantage of experienced professionals where possible, along with having the right ecosystem of partners, will be critical to managing risks and building an effective control environment in a timely manner.



ACROSS THE POND:

A comparison of U.S. and UK cybersecurity risk perspectives

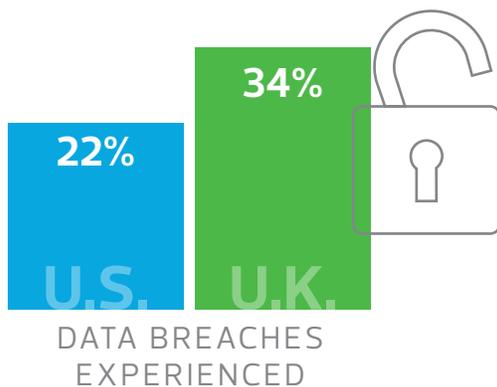


We now live in a global business environment, with middle market companies providing and receiving products and services worldwide. But while understanding risks at home is certainly important, organizations must also know the threats that are prevalent in the countries where they do business.

A significant number of U.S.-based companies have business interests in the U.K. or may be considering future expansion in the region. With data from the RSM UK Middle Market Business Index Cybersecurity Special Report, we can make key comparisons to cybersecurity threats and strategies in the United States and provide insight into how companies may address U.K. risks moving forward.

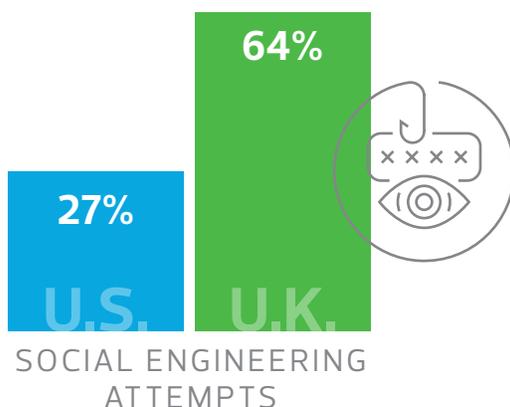
"The United States has lagged behind the U.K. in terms of data privacy for years," commented Stasiak. "However, overall cybersecurity is starting to level out between the two countries."

More breaches occurred in the U.K., but more executives expect attempts in the United States



In the United States, **22% of respondents experienced a data breach in the last year**, while **34% of U.K. executives reported one**. However, **while 72% of U.S. respondents expect unauthorized users to attempt to access data or systems in 2022**, **67% of U.K. counterparts expect a breach attempt**. The risks are high in both countries, but with reported breaches more than doubling in the past year, U.K. companies may need to implement additional controls or adjust cybersecurity strategies.

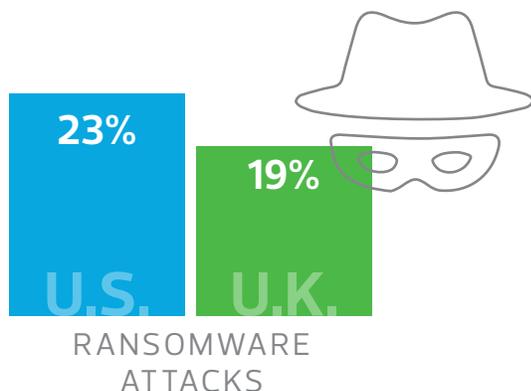
U.S. companies experienced more business takeover attempts, but criminals were more successful in the U.K.



Forty-five percent of U.S. respondents had outside parties attempt to manipulate employees by pretending to be trusted third parties or company executives, **with 27% of those companies ultimately suffering successful attacks**. **Meanwhile, 39% of U.K. companies reported a manipulation attempt, but 64% of those organizations experienced a successful attack**. The manipulation attempts and successful breaches were both down in the United States this year, while the U.K. saw significant increases in both metrics. More U.K. companies provide training, but with attacks on the rise and more of their employees acting on fraudulent requests, more or more targeted training may be necessary.

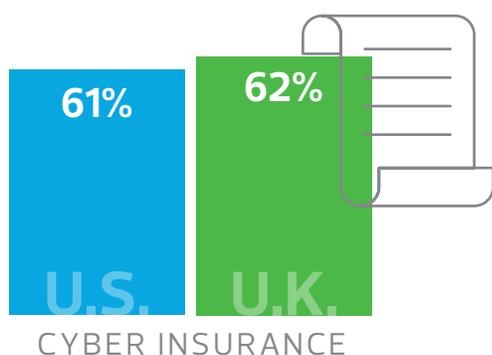
U.S. AND UK CYBERSECURITY RISK PERSPECTIVES, CONT.

The ransomware threat is more pronounced in the United States—for now.



More middle market executives in the United States reported a ransomware attack than in the U.K. (23% versus 19%), but the gap is narrowing. We are seeing a shift in both countries, though, but in different directions. Only 11% of U.K. middle market organizations reported an attack in last year's data, while U.S. executives have experienced a drop from 33% in 2021. In addition, **more U.K. companies expect an attack in the coming year (72% compared to 62%)**. Ransomware cases had been steadily on the rise in the United States before this year's data, and unfortunately, it was only a matter of time before the threat became more pervasive in the U.K.

Cyber insurance is now more extensively leveraged in the United Kingdom.



Cyber insurance became much more popular overseas in the last year, with **slightly more survey respondents now carrying a policy in the U.K. than in the United States (62% versus 61%)**. **The number of respondents whose companies have coverage has stayed fairly consistent in recent years in the United States, but U.K. middle market leaders reported a significant jump**, considering only 40% in last year's report said they carried a policy. Policies have been seen as more restrictive recently in the United States, but U.K. companies are likely now seeing more benefits of coverage as breach attempts continue to increase.

More U.K. middle market companies now leverage the cloud for data security.



In this year's data, **49% of U.K. middle market companies moved or migrated information to the cloud for security concerns, compared to 36% in the United States**. While the amount of U.S. respondents utilizing the cloud for security reasons dropped slightly, the U.K.'s usage grew sharply from 27% last year. An overwhelming number of executives in both countries whose businesses leverage the cloud feel their data is more secure, and U.K. respondents are adopting cloud strategies more often to help address increasing risks.

Organizations with U.S. and U.K. operations must understand the nuances of cyber risks abroad and protections that may be underutilized. With this knowledge, leaders can develop a more effective and comprehensive cybersecurity approach and better protect sensitive data and systems.

Information and data security

The events of the past year are a prime example of the escalating threat of cybersecurity in the middle market. Multiple waves of the COVID-19 pandemic left many employees transitioning between returning to the office and working from home, and created supply chain obstacles across many industries. In addition, the war in Ukraine has created a humanitarian crisis and general uncertainty while further stressing many natural resources, including fossil fuels. These issues have resulted in significant economic tension, requiring many companies to revisit strategies and make adjustments to keep business moving forward.

While these challenges have come together and required significant attention from employees and changes to operations, they have also provided cover for cybercriminals to launch attacks designed to exploit vulnerabilities and control gaps. From amateur hackers to hacktivists and state-sponsored attacks geared toward retaliation, the threat environment is not expected to ease anytime soon.

The recent RSM MMBI survey shows that while cybersecurity remains a pervasive threat, the protective strategies employed by the middle market appear to be working more effectively than in the past. For example, the number of executives whose companies suffered a breach over the last year dropped for the first time since RSM began collecting data in 2015. Twenty-two percent

of respondents reported a breach in this year's survey, compared to 28% in 2021.

Both smaller middle market organizations (16% in 2021 to 12% in 2022) and their larger counterparts (42% to 30%) saw a drop in breaches.

"I think that the larger middle market companies have been exponentially adding multifactor authentication," said Ghazi. "I believe the drop in breaches is a result of having better identity and access management controls in place. It's moving in the right direction."

Despite the decline in successful breaches, middle market executives appear to understand that

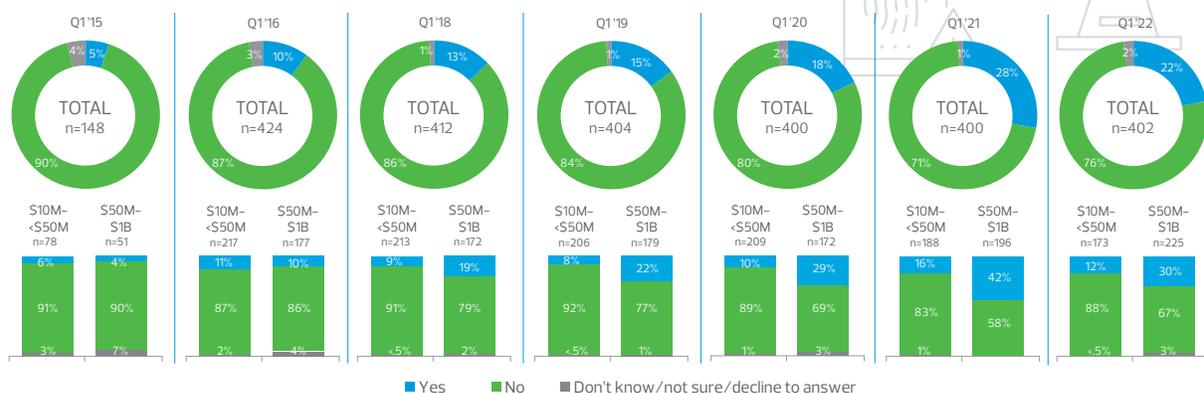
BREAKING THE LOCK

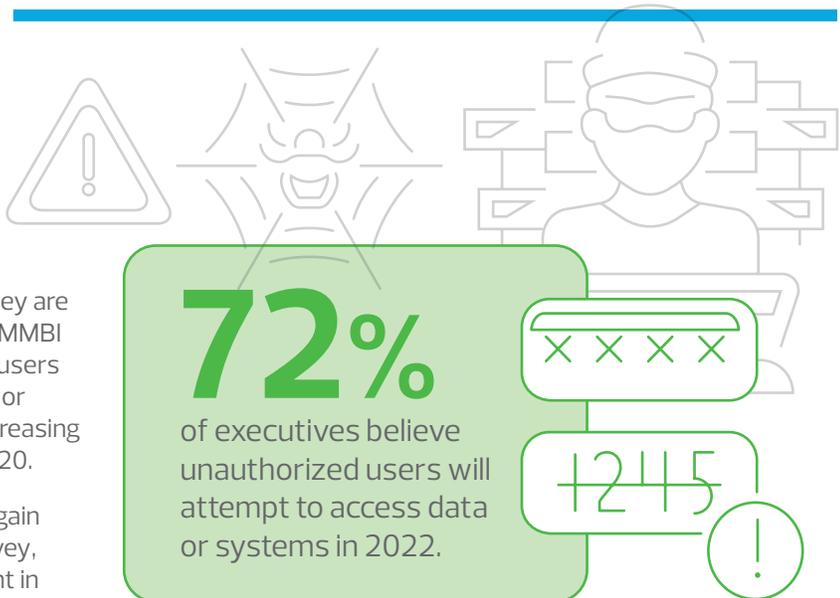
"You're not going to stop the bad guys. You just hope and pray that it doesn't happen. I had a staff member say, 'Well, why would anybody want our data?' Well, they don't know that there's nothing behind the door. They're going to try to break the lock. Even if there's nothing behind the locked door, well, they're still going to try to get that lock off."

NONPROFIT EXECUTIVE

EXPERIENCED DATA BREACH IN LAST YEAR

(BASE = total sample)





cybersecurity risks are not slowing down, and they are now just a part of doing business. In fact, 72% of MMBI survey participants indicated that unauthorized users are somewhat likely or very likely to access data or systems in 2022. That represents a new high, increasing from 64% last year and 55% in both 2019 and 2020.

72%
of executives believe unauthorized users will attempt to access data or systems in 2022.

Confidence in cybersecurity strategies is once again very high in the middle market. In this year's survey, a record-high 96% of respondents were confident in their current measures to safeguard data, up from 93% last year. Companies are making investments in cybersecurity, and they obviously feel like they are making the right moves.

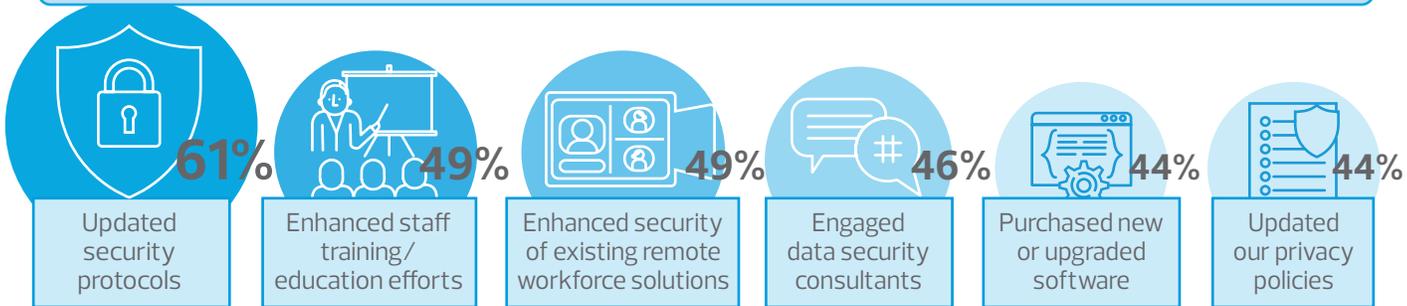
focused on data security and privacy, down from 71% in the previous two years.

"Companies, cloud providers, consulting firms and technology providers have all been making inroads to make it difficult for cybercriminals to access data and systems," commented Ghazi.

"Middle market companies are increasingly interested in exploring managed security services and outsourcing their security monitoring processes," Ghazi said. "It is getting clear to middle market companies that building this competency in-house is not a cost-effective proposition and never amounts to the quality or rigor needed to perform this function properly. Managed security service providers have established a method of building the appropriate skills and scalable technology platforms for such operations; hence, outsourcing these functions has become extremely attractive."

One of those cybersecurity strategies often seen in the middle market is an increased reliance on managed security services. That is demonstrated by a drop in organizations with an in-house security and privacy presence in the MMBI data. Sixty percent of middle market executives report having a dedicated function

Top six actions taken due to publicized data security breaches





"Middle market companies are increasingly interested in exploring managed security services and outsourcing their security monitoring processes. It is getting clear to middle market companies that building this competency in-house is not a cost-effective proposition and never amounts to the quality or rigor needed to perform this function properly"

Tauseef Ghazi

National leader of security and privacy services
RSM US LLP



Organizations took a wide variety of actions in response to publicized data security breaches in the past year, and many changed existing processes. The largest number of MMBI respondents reported updating security

protocols (61%) over the past year, which was consistent with last year's data. In addition, nearly half of the executives reported enhancing the security of existing remote workforce solutions and strengthening staff training and education efforts (49% each).

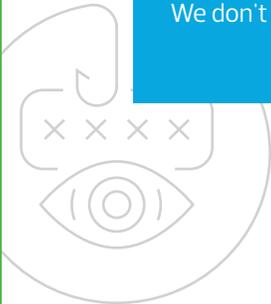
LEVERAGING OUTSOURCING TO KEEP PACE



"Outsourcing is our best way to afford the expertise for cybersecurity or anything else revolving around IT today. The landscape is changing so fast in cybersecurity that staying on top of it, it's just really not possible for us internally. We don't have the resources to stay on top of it."

MANUFACTURING EXECUTIVE

With a confluence of significant challenges over the past year, middle market companies have had more to manage from a cybersecurity risk perspective than ever before. But after years of increases in reported data breaches, this year's drop is welcome news. However, the criminals won't stop their unrelenting efforts to illegally access systems, and they will only get bolder as time goes by. Cybersecurity controls and strategies have come a long way in the middle market, but that progress must continue to keep pace with evolving threats.



Cyber insurance

Cyber insurance is evolving as cybersecurity risks have become more prevalent and breaches have become more costly. Finding the right level of coverage is still a key element of the risk management approach for the majority of middle market companies; in many cases, policies have become more difficult to obtain, while premiums are increasing to match the level of risk for carriers.

The number of stories grows daily. A well-defined cyber insurance policy can help organizations recover quickly from a breach and secure critical systems and sensitive data. If a middle market company has not yet needed direct support from a cyber insurance provider, they at least know a peer that has narrowly avoided disaster, thanks to the timely response by insurers in the critical hours following a breach. However, with the changes in the market, companies must be sure that their controls keep up with insurer expectations to qualify for a policy and that they understand their coverage levels.

LOST COVERAGE FOLLOWING A BREACH



"They (insurance) covered all the consulting we had to bring in; they covered our labor, they covered some of the tenets we brought in to supplement recovery. However, we actually had to get a new policy because our carrier would not renew our policy. You would think they would think more strongly about us."

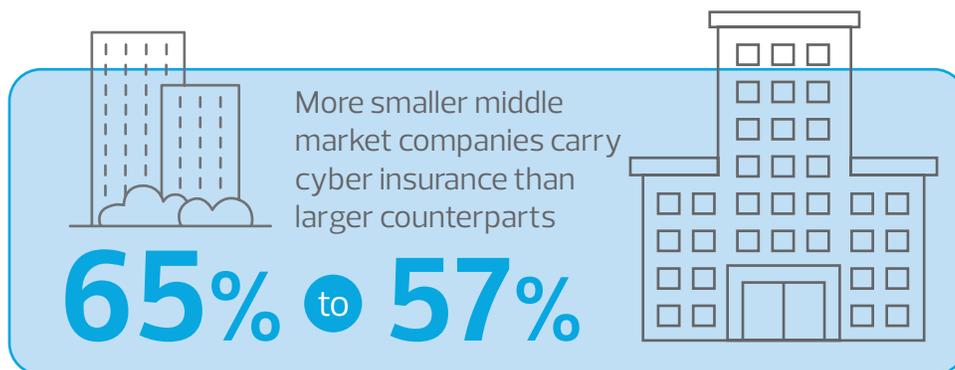
SPECIALTY CONTRACTING EXECUTIVE

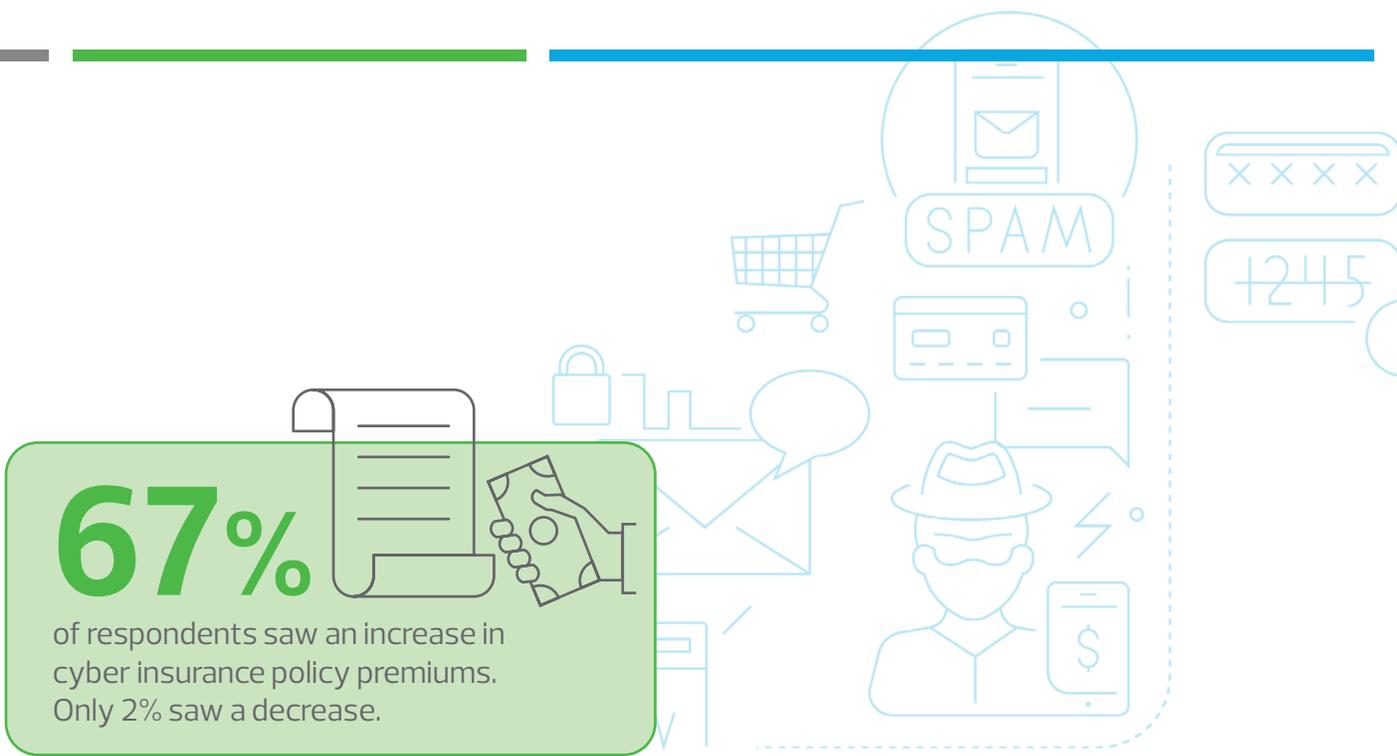
The RSM survey found that 61% of respondents currently utilize a cyber insurance policy to protect against internet-based risks, falling slightly from 65% in last year's report. Looking more closely at the data, the number of smaller middle market companies with cyber insurance increased to 65% this year from 59% in 2021, while larger companies that reported carrying a policy actually fell to 57% from 71%.

"Cyber insurance has gotten very expensive," said Ghazi. "Middle market companies have to weigh their options and whether to stick with higher premiums or potentially self-insure. Instead of paying the rising premiums and potentially paying out of pocket anyway for overages in a significant breach, some are deciding that they will risk paying the related costs themselves."

Cyber insurance is designed to work in conjunction with traditional insurance coverage, which does not often offer options for internet-related risks. In fact, many insurers do not offer cyber liability coverage because they have not collected and analyzed enough data in the area compared to more mainstream risks, and therefore, confidently assessing threats can be difficult. That is why premiums and coverage levels can vary significantly from year to year, and companies must understand the details of their policies and where any gaps may exist.

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, two-thirds (67%) of respondents reported increased policy premiums compared with their prior period, with only 2% seeing a decrease.





67%

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

"Yes, the costs have risen given the amount of payouts, but the availability of insurance has also been greatly affected," commented Stasiak. "We are hearing countless stories about companies that are being turned down, given the risks and their overall profile."

However, along with generally increasing policy rates, it appears that more risks are being covered for most middle market companies. The MMBI research shows that 52% of respondents saw covered risks increasing either somewhat or significantly in their new policy period. The increase is more pronounced for larger middle market companies, with 66% seeing more extensive coverage, compared to 34% of smaller organizations.

In this unstable insurance environment, it appears that middle market companies are generally taking the initiative to understand what their coverage entails. Among middle market companies that carry cyber insurance policies, 67% of executives reported they are familiar with their coverage, a slight increase from 64% last year. Awareness of coverage for larger middle market companies stayed consistent at 80%, while smaller companies increased to 53% from 49%.

"As cyberattacks rose in 2021, people became more cautious," commented Ghazi. "People were more focused on understanding what was in their cyber insurance policies and working through them. The rise in premiums for cyber insurance is also prompting many middle market organizations to take a closer look at their policy and the stipulations they need to adhere to."

Cyber insurance policies tend to have several coverage options that can be joined together to develop a comprehensive policy based on a company's specific needs. It's no surprise that coverage for extortion (including ransomware attacks) was most prevalent among executives in this year's MMBI survey, with 64% choosing that option compared to 47% last year. The jump was even more pronounced among larger middle market companies, increasing to 61% from 39% in 2021, while smaller organizations moved to 70% from 66%.

Much of the other coverage that middle market companies are utilizing is similar to last year, including data destruction (63%), hacking (62%), theft (62%), business interruption (56%) and post-incident investigative expenses (54%).

While cyber insurance has become more expensive and potentially more restrictive to meet the demands of the current risk environment, it is still an extremely valuable protective tool for many middle market businesses. If a breach occurs, an effective policy can help to significantly lessen the financial, reputational and regulatory impact and hasten the recovery process. However, as with any insurance product, companies must be careful when choosing coverage areas and limits to ensure that the policy delivers on its expected value.



Ransomware attacks

As in other segments of the economy, ransomware attacks remained the main cybersecurity threat to the middle market. Many of these attacks often do not require a high level of effort and represent a low-risk, high-reward opportunity for cybercriminals to take control of critical systems or sensitive data and demand large sums of money for their release.

If successful, a ransomware attack can require significant effort and cost to remediate while simultaneously stifling business productivity. With these challenges in mind, identifying and containing potential ransomware attacks must be a top priority within any middle market cybersecurity strategy.

An attack can take many forms, which requires a high level of awareness throughout the organization, including employees at all levels. For example, the most common attack involves fraudulent emails sent to users from a fake or compromised email address presented as a legitimate message to provide or ask for information about the company or an individual. Other breaches are more sophisticated, specifically targeting users, networks or systems that have been identified as vulnerable.

In the early days of the COVID-19 pandemic, criminals were quick to strike as many employees transitioned to a work-from-home environment, and data became increasingly decentralized. While companies have done a much better job securing remote environments as time has gone by, potential network intruders are quick to

FOREIGN SERVERS

"In the last year, cybersecurity has become a very big concern. We were actually hit with ransomware about a year ago. We couldn't pay it. They had foreign servers in a country where the U.S. doesn't allow money to be sent. For a while, we thought we'd have to rebuild from scratch, but we were eventually able to reach around our code and get a backup we could work with. We didn't know who our employees were or how we were going to pay people—our entire network was corrupted."

SPECIALTY CONTRACTING EXECUTIVE

pivot to current issues or seemingly legitimate-looking company information that might strike a chord with users and convince them to click an infected link.

Regardless of the message, once cybercriminals gain access to a network, they restrict access to specific files or entire segments of a network. A message is distributed with details about the locked locations and specific ransom demands to unlock them before they are destroyed. At this point, companies typically have two options: pay the ransom or attempt to regain access to the files on their own or with help from a third party. Either way, the process is often costly.

SAVED BY SYSTEM UPGRADES

"We did get hit with ransomware about a year or so ago. Once we found the attack, we just shut everything down. We went back and deleted everything that was on our network and to the last safe spot on the cloud. We reloaded our systems and basically figured out what wasn't entered and what data was lost. We resurrected that data, and were back up and running pretty quickly. If we had been on our old systems, we would have been toast."

MANUFACTURING EXECUTIVE

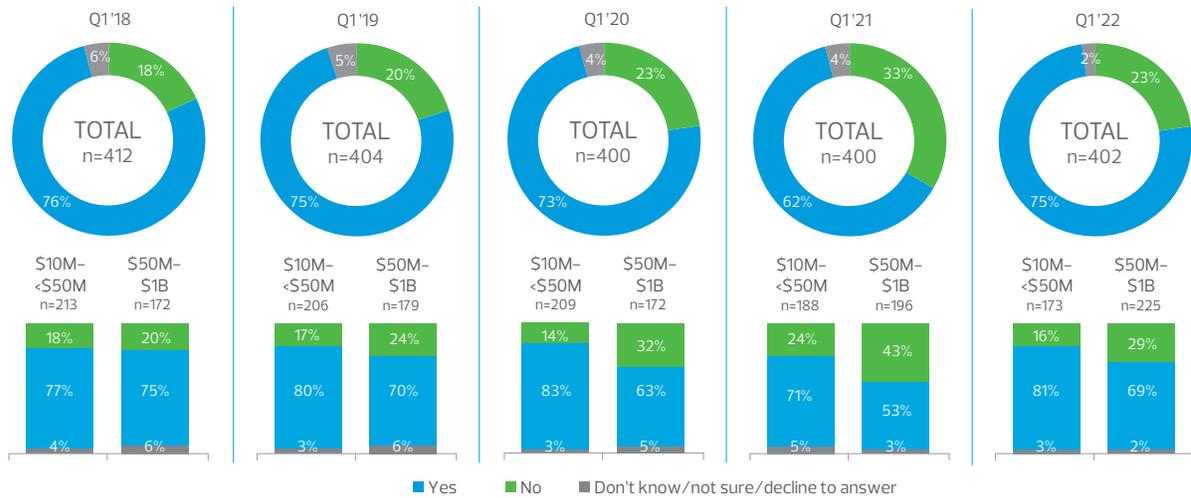
Despite this heightened threat environment, MMBI survey respondents reported a drop in ransomware attacks and demands for the first time since RSM began collecting such data in 2018. Twenty-three percent of middle market executives disclosed that they experienced a ransomware attack or demand in the past year, down from 33% last year. Larger middle market companies reported a bigger drop in attacks with 29% this year compared to 43% in last year's report, while 16% of smaller organizations suffered an attack or demand in contrast to 24% in 2021.

Once again, Ghazi sees an improvement in controls and a shift in strategy as the catalyst in the drop in ransomware attacks.

"Companies are implementing multifactor authentication, utilizing more outsourcing and relying on third parties to provide security services," he said. "In the past, there was no endpoint protection and monitoring happening within

EXPERIENCED A RANSOMWARE ATTACK OR DEMAND DURING THE LAST 12 MONTHS

(BASE = total sample)



middle market companies—that was always reserved for larger organizations, given such technologies are not cheap. Now with the introduction of middle market-specific managed security services, costs are reducing, and there is good progress being made, especially in the upper tier of the middle market."

The number of respondents in the MMBI research who know a peer whose company suffered a ransomware attack stayed consistent in 2022 compared to recent years. In this year's survey, 41% reported that they know someone whose firm has been the target of an attack, compared to 42% last year and 41% in 2020.

As the number of attacks drops, middle market leaders know that the ransomware threat is not going to diminish in the near future. In fact, the number of MMBI survey respondents who believe they are at risk for a ransomware attack in the next 12 months increased—to 62% from 57% last year. Seventy-one percent of respondents from larger middle market companies feel that they are at risk for a potential attack this year, compared to 49% of smaller companies.

Given their potential for high rewards and relative ease to deploy, ransomware attacks will continue to be a significant threat in the middle market for quite some time. However, the middle market is certainly making progress and taking effective steps to reduce the frequency and severity of attacks. Companies cannot be happy with those advances and become complacent, though, as countless cybercriminals are ready and waiting for any opportunity to strike.

A FORTUNATE CHANGE IN SYSTEMS



"We recently suffered an attack that originated from Russia. They got into our servers and compromised many files, then required a key. They demanded \$200,000 in bitcoin for the key, and the ransom would double to \$400,000 in seven days. We did not pay and reported the breach to the FBI, state police and local police. We had insurance coverage, and they put us in touch with a company that diagnosed the attack, helped us go to our backups and get files that were not corrupted.

The night before the attack, we sent our accounting files to a new company in preparation to move to a new accounting system. We would have been in trouble if that had not been in the works. It was a pain, and crimped operations for a few weeks, but we were able to keep trucks dispatched and recreate things on the accounting side."

PETROLEUM COMPANY EXECUTIVE

Business takeover threats



Much like ransomware, business takeover attacks require very little effort and sophistication on the part of criminals, and therefore, they will likely be a perpetual threat to the middle market. However, no matter how simple, a successful attack can be very harmful and difficult to detect because it can be carried out by almost anyone. The most common forms of business takeover attacks are social engineering and employee manipulation—both low-tech cyberattacks, but ones that can result in significant damage.

Social engineering is a popular attack strategy, mainly because of the low level of expertise necessary. In many cases, someone will contact an employee—by phone, email or even in person—and attempt to convince them to provide sensitive data or access to that data. The attacker often poses as a coworker or trusted third party to give the employee a false sense of security. Many of these takeover criminals are very skilled in identifying and exploiting any potential lack of security awareness.

However, the most common business takeover strategy is phishing. Hackers will develop a profile of information from publicly available company data or social media profiles and create messaging that is designed to look like it is from a friend or coworker. Those sometimes carefully, sometimes crudely crafted messages attempt to convince users to click on a corrupt link or attachment.

The COVID-19 pandemic also brought a resurgence in fraudulent emails that continues today. Throughout the pandemic, emails flooded inboxes to capitalize on fear and panic, promising information on vaccines, the spread of the virus or charitable efforts—all with links to malware or malicious code. While those emails have subsided, people will likely continue to see messages

designed to look like appeals for humanitarian aid during global conflicts or other times of tragedy.

The reported frequency of business takeover attempts has remained fairly consistent over the last few years, and the 2022 MMBI data is no different. Forty-five percent of middle market executives said that outside parties attempted to manipulate employees by pretending to be trusted third parties or company executives, compared to 51% in 2021 and 49% in 2020.

In addition, respondents from smaller companies reported more of these attacks than those from larger organizations, 51% versus 40%, respectively.

All told, middle market executives in the RSM survey reported that 27% of those attempts to manipulate employees were successful over the last year, a considerable drop from 45% in 2021's data. Larger middle market organizations showed the largest decrease, reporting a 38% success rate for attacks, compared to 67% just last year.

"The upper-middle market appears to be doing a better job at training their people," said Ghazi. "The lower-middle market is likely seeing an increase in attacks because attackers are shifting their focus after not being as successful with larger companies."

While business takeover attempts became less successful in the middle market, there is no end in sight to the potential threat. In the MMBI study, 73% of executives said their organization is at risk of an attack by manipulating employees in the next 12 months, a slight increase over last year and the highest number ever recorded. The number of smaller organizations expecting an attack rose to 68% from 59% last year,

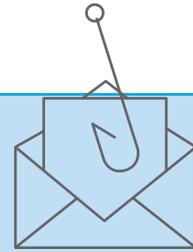


while executives from larger organizations that believe a takeover attempt is likely fell slightly to 78%.

With business takeover attacks capable of coming from many angles, middle market companies need to utilize several strategies to address them. Of the organizations in RSM's survey that had unsuccessful attacks, 76% listed employees not acting on the fraudulent request as a reason for the failed breach, a 12% drop from last year's survey. In addition, 65% of middle market executives said that secondary controls prevented the completion of an attack, and 53% acknowledged system controls that prevented delivery of fraudulent communications or materials to employees.

At the end of the day, training is typically the best defense against business takeover attacks, providing real-life examples of how criminals may attempt to manipulate employees. The overwhelming majority of survey respondents see the value in training, as 89% of executives reported their organization provides training to at least some employees on how to detect, identify and

45%



of respondents said that outside parties attempted to manipulate employees by pretending to be trusted third parties or company executives.

27% of those were successful over the last year, a drop from 45% in 2021.



prevent attempts to gain unauthorized access, consistent with last year's data.

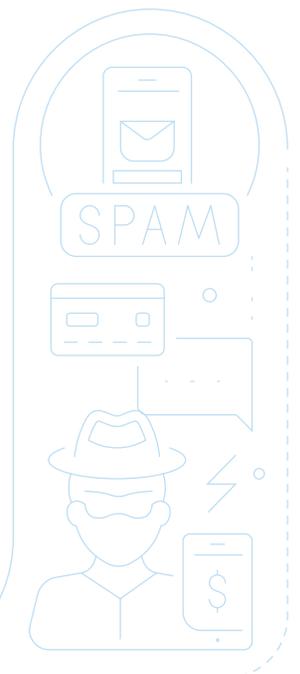
With business takeover attacks not requiring a significant amount of technical proficiency or effort to carry out, they will remain a part of the cybercriminal's playbook for quite some time. Middle market companies have made progress by understanding the threat at hand and implementing protective controls, but those steps must continue and evolve along with threats moving forward.

LEGIT OR NOT?



"Our provider tests us constantly, pinging our staff with phishing emails to see if they fall for it. If they do, they have to watch a video about what you need to look for and how to avoid it. We're down to maybe a 5% failure rate. When we started testing, seven or eight years ago, it was over 50%. We have trained our staff, it's easier to spend 30 seconds really looking at an email and saying, 'Is this legitimate?' than watching the instructional video."

NONPROFIT EXECUTIVE



Privacy protections compliance

While cybersecurity is an ongoing priority for the middle market, companies cannot lose sight of progressive legislative efforts toward enhanced data privacy. Data is a critical commodity for middle market companies, providing the foundation for key operational decisions and the development of products and services. But an increasing number of data privacy standards from overseas and within individual states have changed the focus from how data is secured to why companies have it in the first place.

The European Union's General Data Protection Regulation was developed and implemented in 2018 and has served as the model for several subsequent data privacy standards worldwide. The GDPR established guidelines for how companies transmit, process and hold EU resident data, regardless of whether they have European operations or not. While companies outside of Europe were generally slow to adjust to the GDPR, several high-profile enforcement actions led to compliance becoming much more common.

Following the success of the GDPR, data privacy standards have slowly made their way to the United States. As of early 2022, at least 16 individual states have implemented some form of data privacy laws, including

comprehensive standards in California, Colorado and Virginia.

For many years, a federal data privacy standard has been discussed in the United States and has often appeared as a "not if, but when" scenario. Despite bipartisan support, momentum for a potential federal law has appeared to stall, although it could pick back up at any time. Without a nationwide standard, the data privacy landscape may actually be more challenging for businesses, as they have to contend with a patchwork of state regulations that will only become more complex as legislation is introduced in additional states.

"Currently, in the U.S., data privacy is a state-level issue," said Ghazi. "It was very noisy in previous years where privacy was becoming a big debate, but garnering support for overarching privacy legislation at the federal level has been slow-moving in Washington. While it seems that technology-related regulations are more prevalent when a Democratic government is in place, using GDPR as a template model is not considered the right course of action by legislators on both sides. There are also concerns around superseding state regulations in this space."

"It was very noisy in previous years where privacy was becoming a big debate, but garnering support for overarching privacy legislation at the federal level has been slow-moving in Washington"

Tauseef Ghazi

National leader of security and privacy services
RSM US LLP



Among companies familiar with the GDPR,

90%

believe it is likely that they will have to comply with privacy legislation in the next two years and

96% say that preparing for emerging privacy regulations is a priority.

GDPR

Middle market companies doing business in Europe are subject to GDPR requirements, and awareness of the standard has continued to grow. Fifty-eight percent of executives in the RSM MMBI survey said they are familiar with the requirements of the law, up from 55% in 2021. Consistent with past years, respondents from larger organizations were more familiar with GDPR requirements than those at smaller organizations—80% versus 32%.

As data privacy guidelines spread across a growing number of states, many middle market companies understand they will likely need to adhere to new laws in the near future. Among RSM survey respondents familiar with GDPR requirements, 90% said that their organizations would likely have to comply with privacy legislation similar to the GDPR at a state or federal level in the United States during the next two years, a 2% decrease from last year's data.

With data privacy projected to be a front-burner topic for the foreseeable future, the continued rollout of

legislation by more states, and a federal standard still a topic of discussion, middle market executives are taking data privacy legislation seriously. For example, 96% of executives in the RSM survey who are familiar with the GDPR said preparing for emerging privacy regulations is a priority, almost identical to last year's response. Ninety percent of smaller middle market organizations are prioritizing data privacy preparations, compared to 98% of larger companies.

The wave of data privacy regulations may not have come as quickly as many expected in the United States, but state guidelines are steadily expanding and making operations more complex. Just because a federal standard has not been enacted does not mean that data privacy can be out of sight, out of mind. If companies work with European customers, they are likely subject to GDPR requirements, and if they have customers or contacts in multiple states, chances are increasing by the day that complying with state guidelines is necessary.

Migration to the cloud to ensure data security

The cloud has been an extremely valuable tool for the middle market for many reasons, and at this point, almost every company uses the cloud in some way. Many organizations initially moved files and systems to the cloud to decrease reliance on on-premises servers and increase access and visibility to key data. But companies have found that the cloud is also an effective security tool. With economies of scale, cloud providers can deliver enhanced controls and security capabilities that are often out of reach for many middle market organizations.

The RSM MMBI data shows that 36% of middle market companies moved or migrated data to the cloud as a result of security concerns during the past year. That represents a drop from last year's data when 40% reported transitioning data to the cloud. Thirty-three percent of smaller middle market companies reported a move to the cloud for security reasons, a slight increase from last year's 26%. However, larger middle organizations reported a sizable decrease, with 39% transitioning to the cloud over the past year, compared to 53% in 2021's data.

FROM SERVER ROOM TO LIVING ROOM



"With the move toward the cloud, you're taking that onus of security off that in-house server and putting it on somebody like Microsoft, who you've got to trust is doing a lot better job than you were with that server stuck in a closet. So that has changed the security game; I want to go put a La-Z-Boy in our server room because there's nothing in there."

NONPROFIT EXECUTIVE

"Moving to the cloud was a huge concern for the last two years," commented Ghazi. "Many middle market companies have already moved to the cloud, and they continue to move. During the pandemic, the technology became more available because people needed it. It's no longer a two-to-three-year journey to the cloud; providers worked through more efficient processes, and now a transition can happen much faster. That said, those moves come with additional cyber risks that need to



90%

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

be considered proactively. No two cloud environments are equal, so the security and architecture of your cloud environment need to be understood."

As in past years, the overwhelming majority of companies leveraging the cloud to strengthen security are seeing results. Among middle market executives who reported moving data to the cloud for security concerns, 90% believe the data residing in the cloud is more secure. That represents a small increase from last year's survey (88%).

While the cloud does typically lead to stronger controls for data and applications, that security often comes at a higher cost. The RSM survey finds that 75% of middle market executives said that storing data in the cloud for security reasons was more expensive, nearly identical to last year's survey (76%). Conversely, 19% of respondents disclosed that moving to the cloud for enhanced security was less expensive, also similar to last year's data (21%).

With the majority of companies utilizing the cloud to some extent, it is worth evaluating how much it could potentially enhance the security approach of middle market organizations. Much like it has been used to take the pressure off internal personnel to maintain internal servers, it can also combat persistent security threats by enabling advanced controls and redundancy that may not always be realistic with in-house solutions. While it likely will come at a higher cost, the value gained from avoiding a potential breach is difficult to quantify.

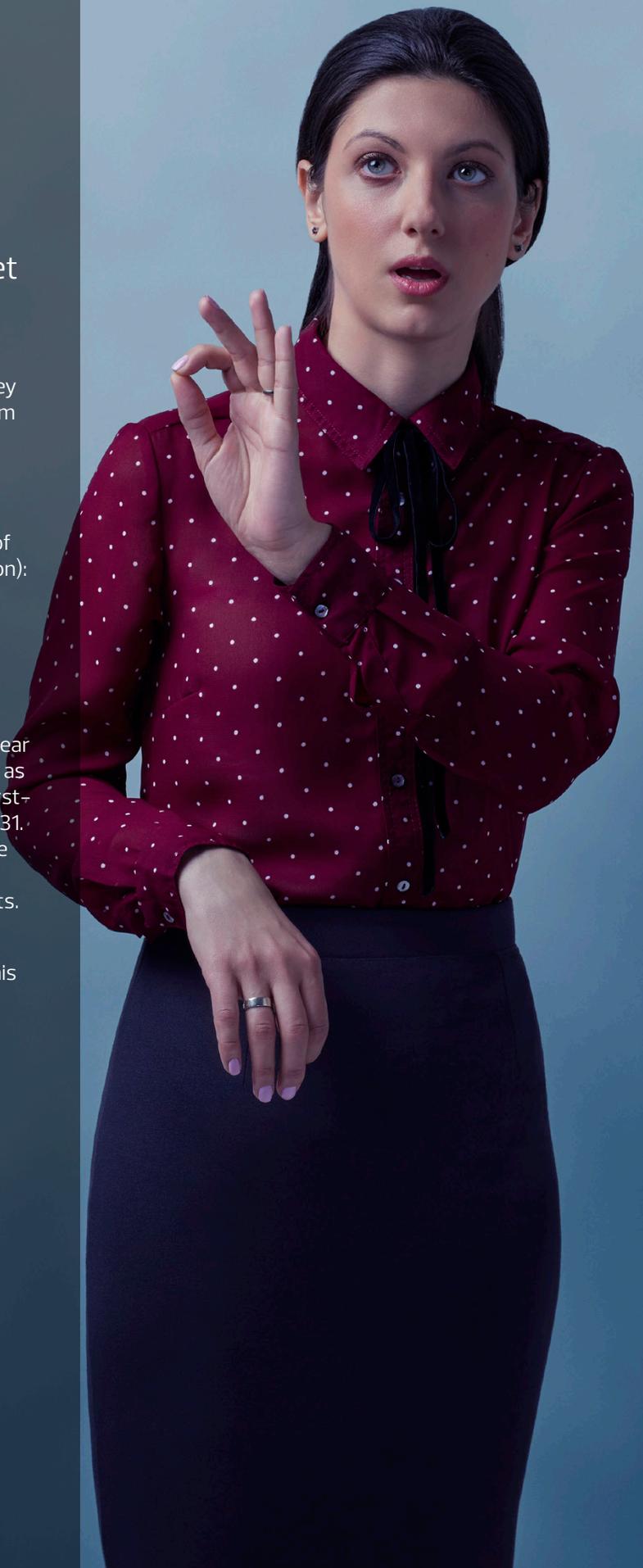
Methodology

About the RSM US Middle Market Business Index research

The RSM US Middle Market Business Index survey data in the first quarter of 2022 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 2022 first-quarter survey was conducted from Jan. 10-Jan. 31. Information was collected by phone and an online survey from 402 executives, including 217 panel members and a sample of 185 online respondents. Data is weighted by industry.

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



Additional reporting requirements planned for critical sectors and public companies



President Biden's \$1.5-billion 2022 omnibus spending bill includes a \$2.6 billion outlay for the nation's cyber defenses, as well as provisions that call for companies to report cybersecurity breaches to the federal government.

The allocation to the Cybersecurity and Infrastructure Security Agency (CISA) is \$568 million above 2021 funding levels and comes amid heightened concerns about U.S. cybersecurity following Russia's invasion of Ukraine.

The omnibus legislation, which passed the House and Senate in mid-March, provides funding for the federal government through September.

The new cyber reporting requirements call for companies in critical sectors such as energy, finance and health to alert CISA within 72 hours of being hacked and within one day of paying ransom as part of a ransomware attack. The information those businesses provide would be anonymized and shared with government, cyber response firms and other relevant stakeholders.*

"While these cyber reporting requirements are limited mostly to larger, critical infrastructure entities, middle market companies must remain on alert as similar, previous proposals including broader market segments could very well resurface in the future," says Dan Ginsburg, RSM public policy leader.

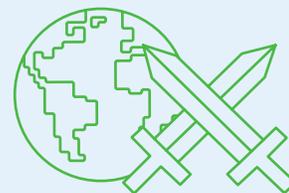
Companies that fail to report their cyber incidents under the new legislation would be subject to subpoena by CISA, a division of the U.S. Department of Homeland Security created in November 2018. In exchange for cooperation in reporting, the government will offer limited liability protections.

In addition to provisions in the spending bill, the Securities and Exchange Commission has issued new proposed rules that will have a significant effect on public companies. The proposed standard is designed to address inconsistencies in cyber incident reporting, and will require registrants to disclose information about a cybersecurity event within four business days of an incident with a material impact on the business.

While public companies should keep an eye on the progress of the proposed rule, private companies should take note as well. Even though the rule is designed for public entities, similar standards often follow closely for private companies. Regardless, increasing accountability is always a best practice and can help lead to more effective controls and identify weaknesses before they lead to a potential breach.

**None of the reporting requirements will take effect until CISA implements rulemaking procedures.*

Managing cybersecurity threats related to global conflict



Global tensions are on the rise, and cyberattacks are increasingly used as weapons by nations or by hacktivists who support a specific cause. For example, during the war in Ukraine, the Cybersecurity and Infrastructure Security Agency (CISA) warned that every U.S. organization is at risk from cyberthreats that can disrupt essential services and potentially result in harm to public safety.

Global conflicts are unfortunately going to continue to occur, and organizations, regardless of size, should remain on heightened alert for retaliation from cyber actors from within involved nations, as well as others who may take advantage of the situation, and they should ensure the implementation of key defenses.

The following are examples of activities that can increase resiliency and reduce the risk of suffering severe consequences from a targeted attack. In addition, organizations should adopt a risk-based posture that evolves with the changing threat landscape.

- **Cyber resiliency**—have an established business continuity plan and maintain an inventory of systems and their established criticality, allowing for decisions to be made by prioritization. Review or develop playbooks for warzone operations, conduct tabletop exercises and test backups for critical assets.
- **Crisis communications**—establish internal communication procedures, including consistent expectations of regular updates and rapid messaging to employees. External communications should focus on brand protection, engaging with a public relations firm if necessary.
- **System and software updates**—ensure all systems and software remain up to date, prioritizing updates that address [known vulnerabilities](#).
- **Extended detection and response**—ensure that endpoint and network protection solutions are installed on all devices, remain up to date and monitored for unauthorized changes.
- **Increase maturity of identity and access management (IAM)**—reduce the attack surface

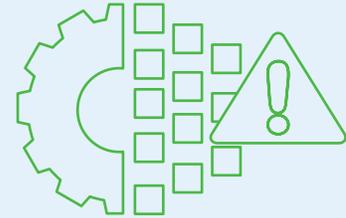
by utilizing the principle of least privilege, including the review and removal of unnecessary administrative rights for users and/or shared administrative passwords across devices. Confirm that alerting is configured to detect changes within the IAM system, including privilege escalations and role changes. Utilize multifactor authentication, where possible, on externally accessible systems, such as email, portals and remote access technologies.

- **Security awareness training**—enhance employee training, confirming that employees are aware of current common threats and how they are delivered. Establish blame-free employee reporting, ensuring that employees know who to contact during an instance of suspicious activity.
- **Review third-party relationships**—identify critical vendors with operations in affected areas, ensure that you understand their contingency plans and that they are properly managing their cybersecurity risks. Review contractual language to ensure that it includes appropriate security controls and requirements and document current inventory levels, including on-site and in-transit materials, identifying alternate sources as appropriate. Identify alternate providers as appropriate.
- **Maintain operations**—from a business perspective, review staffing plans for locations affected by the current conflict to maintain critical operational activities. Consider retaining outside legal counsel focused on the continuity of processes.

While middle market companies are implementing a wide variety of protections and controls to combat cybersecurity risks with increasing levels of success, Tauseef Ghazi, RSM national leader of security and privacy services, offers a word of caution about the importance of awareness as tensions escalate.

“The more controls that you have in place, the harder it is going to be for criminal organizations,” he said. “But as you make it more difficult for them to get through, they will become more reckless. As you put them into a corner, they are going to find other ways to retaliate.”

Understanding cybersecurity risks related to digital transformation



Digital transformation is a term that has become very popular in the middle market, with organizations establishing plans to replace aging technology systems and embracing innovations that promise greater insight, productivity and efficiency. And while new platforms can certainly have a positive influence on business operations, any abrupt changes can also create vulnerabilities and control gaps that can be exploited by cybercriminals.

For example, almost every middle market company now uses the cloud in some form to house data and applications. While the cloud does have some well-documented advantages over on-premise servers, managing the new environment involves different processes and organizations are not always prepared.

"For a middle market company, the cloud does add a lot of new capabilities," said Tauseef Ghazi, RSM national leader of security and privacy services. "But it also gives you a lot more to manage and it does involve new risks. For a company that has not been there before, those risks could be ones that they are just not proficient enough to understand or mitigate just yet."

Ken Stasiak, RSM national leader of cyber testing and response, detailed how the cloud—and its potential challenges—have evolved. "Moving to the cloud a few years ago was pretty simple," he said. "You had three options. Today, cloud providers offer more options, and it's easy to forget to turn one of these options on or off."

In addition to the cloud, companies are constantly evaluating new customer relationship management and enterprise resource planning solutions, as well as a host

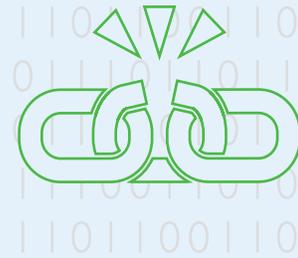
of big data and automation applications. And we have yet to scratch the surface of the connectivity and efficiency potential of the Internet of Things. But each of those implementations introduces new access points and new data sources, and organizations need to connect the dots to keep the business safe.

New technology investments also typically mean working with new third-party vendors. Companies must carefully evaluate vendors and their policies for protecting data, as many of the most significant breaches over the last few years were due to vulnerabilities or inadequate vendor controls.

"Digital transformation is now an essential strategy for success in the middle market," commented Bill Kracunas, RSM national management consulting leader. "But any decision to implement a new system or solution must have security in mind. Companies want to take advantage of the productivity, scalability and insight that new innovations offer, but they can't risk leaving themselves vulnerable to a cybersecurity attack in today's risk environment."

Innovation is not slowing down, and middle market companies will continue to look at advanced tools and applications to stay competitive. But they must perform the necessary due diligence to ensure that new solutions designed to take a company to the next level do not actually end up harming the business.

Middle market leaders detail supply chain cybersecurity concerns



During the COVID-19 pandemic, middle market companies saw firsthand how fragile their supply chains could be. While the flow of goods and supplies proved to be vulnerable to many pandemic-related risks, it is also subject to the same cybersecurity threats as other companies. Often, key suppliers are more of a target due to their size and importance.

Considering the recent supply chain challenges and the volatile cyber-risk environment, many middle market companies are understandably uneasy about the cybersecurity standing of their suppliers. In this year's MMBI survey, 55% of middle market executives who carry a cyber insurance policy expressed concern over interruption or delay in receiving products, raw materials or services due to cyberattacks on an upstream supplier. This includes 39% of leaders at smaller middle market companies and 69% at larger counterparts.

In response, those companies are taking several actions, with 52% of respondents maintaining incident response plans that require notification if a vendor's network, systems or data have been compromised or a compromise is suspected. In addition, 50% are monitoring vendor access

to networks and data, 49% train employees on cyber risks specific to their supply chain environment, 42% define data ownership and/or acceptable use requirements, and another 42% monitor vendor compliance with regulatory requirements.

The supply chain is the lifeline of the business. In order to keep key supplies moving, companies should consider taking some of the actions mentioned above or other potential risk identification activities, developing a formal process to evaluate risks within suppliers, similar to a third-party risk program for vendors. This program may include maintaining a log of potential backup companies if an issue occurs at a primary supplier.

As many middle market companies have unfortunately seen over the last two years, any supply chain difficulties can quickly bring productivity to a halt. Organizations should consider any potential steps to prevent disruptions, including those related to the very real risk of a cybersecurity attack.

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

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

For details about RSM US LLP 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.

© 2022 RSM US LLP. All Rights Reserved.



For more information on the U.S. Chamber of Commerce, please visit www.uschamber.com.

For media inquiries, please contact the U.S. Chamber of Commerce at +1 202 463 5682 or press@uschamber.com.

The U.S. Chamber of Commerce is the world's largest business federation representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations.

Copyright © 2022 by the United States Chamber of Commerce. All rights reserved. No part of this publication may be reproduced or transmitted in any form—print, electronic, or otherwise—without the express written permission of the publisher.



U.S. Chamber of Commerce