RSM US MIDDLE MARKET BUSINESS INDEX

CYBERSECURITY

SPECIAL REPORT

U.S. CHAMBER OF COMMERCE

RSM

TABLE OF **CONTENTS**

EXECUTIVE SUMMARY 3

THE THREAT IS INCREASING, BUT THE MIDDLE MARKET IS RESPONDING 9

ACROSS THE POND: A COMPARISON OF U.S.AND UK CYBERSECURITY RISK PERSPECTIVES 12

INFORMATION AND DATA SECURITY 14

CYBER INSURANCE 18

RANSOMWARE ATTACKS 21

BUSINESS TAKEOVER THREATS 25

PRIVACY PROTECTIONS COMPLIANCE 29

MIGRATION TO THE CLOUD TO ENSURE DATA SECURITY 32

METHODOLOGY 35

This cybersecurity special report is in partnership with the U.S. Chamber of Commerce

RSM US LLP (RSM) and the U.S. Chamber of Commerce have joined forces to present the RSM US Middle Market Business Index (MMBI)—a first-of-its-kind middle market economic index developed by RSM in collaboration with Moody's Analytics. Our special reports are derived from a topic-specific question set that varies each quarter.

U.S. CHAMBER OF COMMERCE

RSM

An uncertain environment leads to an unprecedented level of attacks

When it comes to cyberthreats, the old adage held true in 2020: the more things change, the more they stay the same. Hackers and other electronic criminals continued their relentless pursuit of data and sensitive information from middle market businesses, leading to record levels of several types of attacks. The middle market continues to represent a sweet spot for hackers, with companies possessing a significant amount of valuable data, but lacking the level of protective controls and staffing of larger organizations.

The COVID-19 pandemic also altered the threat landscape in the middle market due to the rapid large-scale shift to a remote work environment and more dependency on the internet to remain productive. Many companies simply did not have experience with managing such a transition, and security vulnerabilities—even for a short amount of time—were almost inevitable. Criminals were quick to strike, unleashing a host of attacks ranging from widespread malware and viruses to targeted social engineering and phishing attacks.

After years of increasing breach attempts and successful breaches, the middle market understands the risks that cybercriminals can pose. However, while the pandemic caused a global lockdown and generally kept people at home without the luxury of venturing out to a restaurant or a movie, hackers were locked down as well with little to do but hone their craft and exploit vulnerabilities.

Recognizing and addressing increased cybersecurity risks

Middle market executives provided insight into the rise in data breaches in a recent RSM US Middle Market Business Index survey, while also detailing ongoing cybersecurity concerns and the evolving controls and strategies employed to address security threats and combat hackers.

According to first quarter 2021 MMBI data, 28% of middle market executives claimed that their company experienced a data breach in the last year, the highest level since RSM began tracking data in 2015 and a sharp rise from 18% just last year. Larger middle market organizations were most at risk, as 42% of executives at such companies reported a breach, compared to 16% at smaller counterparts.

The middle market continues to increase investment in a variety of protective measures and 71% of respondents have a dedicated function focused on data security and privacy. However, with the frequency of breach attempts and the ongoing uncertainty and unknown road back to normal in the wake of COVID-19, 64% of respondents anticipate that unauthorized users will attempt to access data or systems in 2021, another significant increase from 55% in both 2019 and 2020.

In this challenging threat environment, cyber insurance should become even more of a priority. The RSM survey found that 65% of middle market organizations carry a cyber insurance policy, a slight increase from last year's 62%. Even more important though was the jump in respondents who claim familiarity with what their policy covers—up to 64% from 48% last year.

28% of middle market executives claimed that their **company experienced a data breach** in the last year

65% of middle market organizations **carry a cyber insurance policy**

Managing an evolving data privacy landscape

In addition to consistently rising cybersecurity risks, the data privacy regulatory landscape continues to shift, and compliance demands are becoming more of a reality for middle market businesses. The European Union's General Data Protection Regulation was implemented in 2018, providing a new standard for how EU resident data is collected and stored. Unlike security guidelines, the GDPR is not focused on how companies secure data, but why they have that data.

The GDPR has inspired several subsequent data privacy regulations in several individual states, including the California Consumer Privacy Act. Over a dozen states have signed privacy regulations into law, and a federal standard is likely on the horizon. During the 2020 presidential election, data privacy was an element of both parties' platforms, but it was a bigger point of emphasis for the Biden campaign. With the middle market's reliance on data to drive decision-making, new laws could require substantial changes to policies and processes.

Awareness is critical with data privacy legislation, and RSM MMBI data shows that 55% of executives are familiar with the requirements of the GDPR, another significant jump from last year's data (39%). In addition, nearly all respondents familiar with the GDPR (97%) indicated that preparing for emerging privacy legislation is at least a priority of minor importance, which is consistent with last year's data.

Utilizing peer data and insight into middle market trends

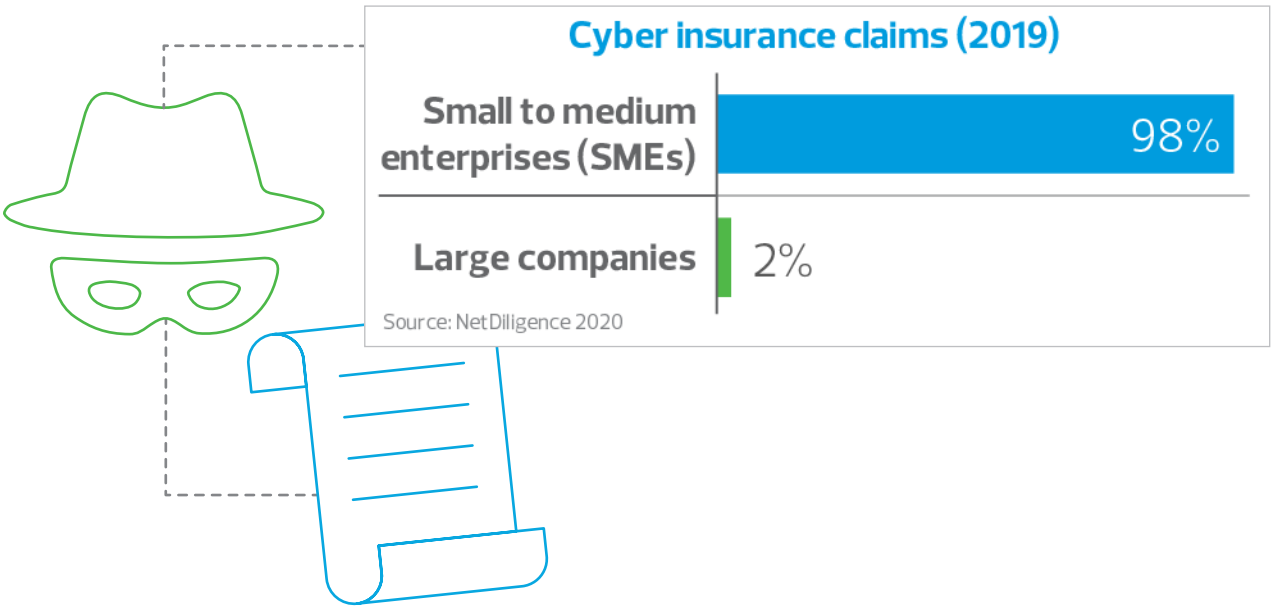
Cyberattacks and breach attempts were already steadily on the rise in the middle market, and the COVID-19 pandemic has only intensified the threat. In this environment, companies must take advantage of benchmarking opportunities and peer insights to develop an effective defensive stance with generally limited resources. RSM has developed this report to provide relevant middle market cybersecurity insights and data privacy trends, as well as to outline strategies organizations can implement to strengthen security and privacy programs.

> While some patterns of cybercriminals are hard to predict, one is highly predictable: when economies and societies go through massive change, bad actors will try to exploit cyber vulnerabilities. Americans have enough to worry about with economic uncertainty, health precautions, job losses, and so forth, and we want to ensure business owners have the right tools to increase the security of their virtual working environments. This annual report provides key data points, recommendations and expert opinions that will help midsize businesses better understand their risk profile and inform their risk management processes.
>
> **Vincent Voci**
> Executive Director, Cyber Policy and Operations, U.S. Chamber of Commerce

NetDiligence research highlights the threat to the middle market

The recent NetDiligence[1] Cyber Claims Study, underwritten by RSM, illustrates how hackers have zeroed in on middle market companies. The report found that 98% of cyber insurance claims came from small to medium enterprises, with only 2% coming from companies with over $2 billion in revenue. The scale continues to tip toward smaller organizations, and the data shows how painful and real the threat has become.

Knowing where to focus protective efforts can often be a challenge for middle market companies, as hackers exploit vulnerabilities that can change over time. For example, the NetDiligence study showed that ransomware was the leading cause of losses among middle market companies, overtaking social engineering, which was the leader in last year's report.



1 NetDiligence is a privately held cyber-risk assessment and data breach services company, utilized by leading cyber liability insurers in the United States and United Kingdom to support loss control and education objectives.

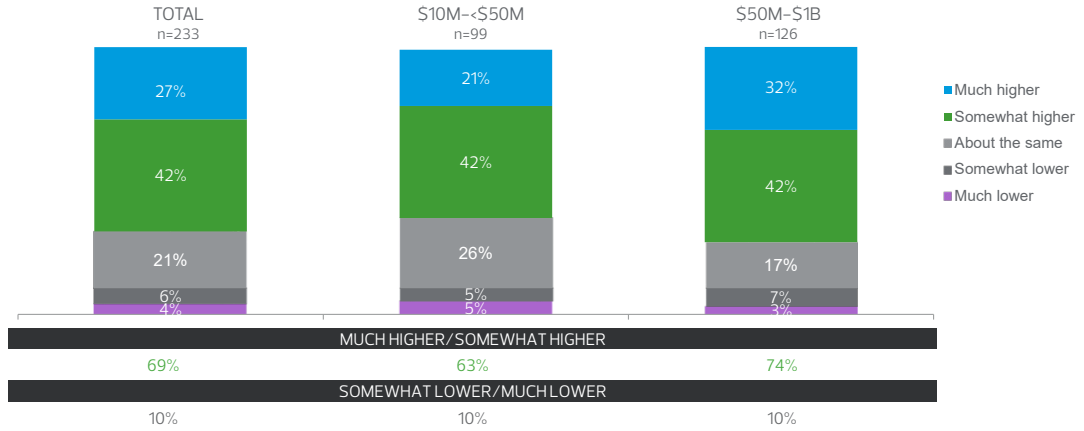
The COVID-19 effect: The pandemic's influence on data security

Not surprisingly, the COVID-19 pandemic had a significant effect on middle market companies' data security efforts over the last year. Hackers have had more susceptible networks to attack, a captive audience and more time on their hands to create chaos.

For example, in the RSM MMBI survey, 33% of respondents reported a ransomware attack in 2020, and 51% suffered a social engineering attack. Of those companies, 69% reported a higher amount of total attack attempts than in 2019. Seventy-four percent of larger middle market companies reported an increase, compared to 63% of smaller companies.

Total number of attacks in 2020 compared to 2019

(BASE = had ransomware attack in last year or outside parties attempted to manipulate employees by pretending to be trusted third parties or company executives)

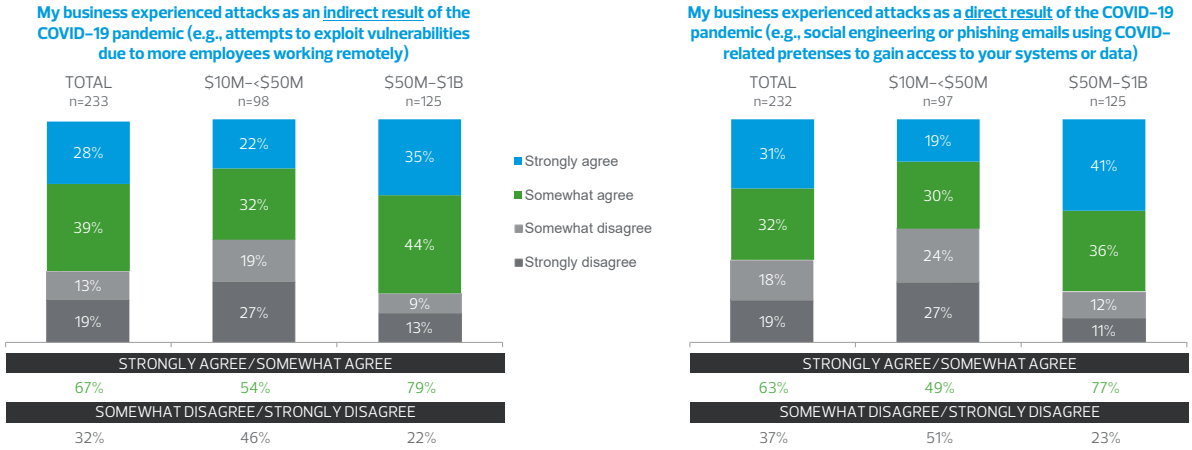


Furthermore, 67% of those respondents who experienced a ransomware or social engineering attack said their businesses experienced attacks as an indirect result of the COVID-19 pandemic. The most common indirect attack would be exploiting vulnerabilities from employees working remotely. A higher percentage of larger middle market companies reported indirect attacks than smaller companies, 79% versus 54%.

By comparison, 63% of those executives reported that they suffered an attack as a direct result of COVID-19, such as social engineering or phishing campaigns based on COVID-19-related pretenses. Once again, larger middle market companies were victimized at a higher rate, 77% compared to 49%.

Level of agreement attacks result of Covid-19 pandemic

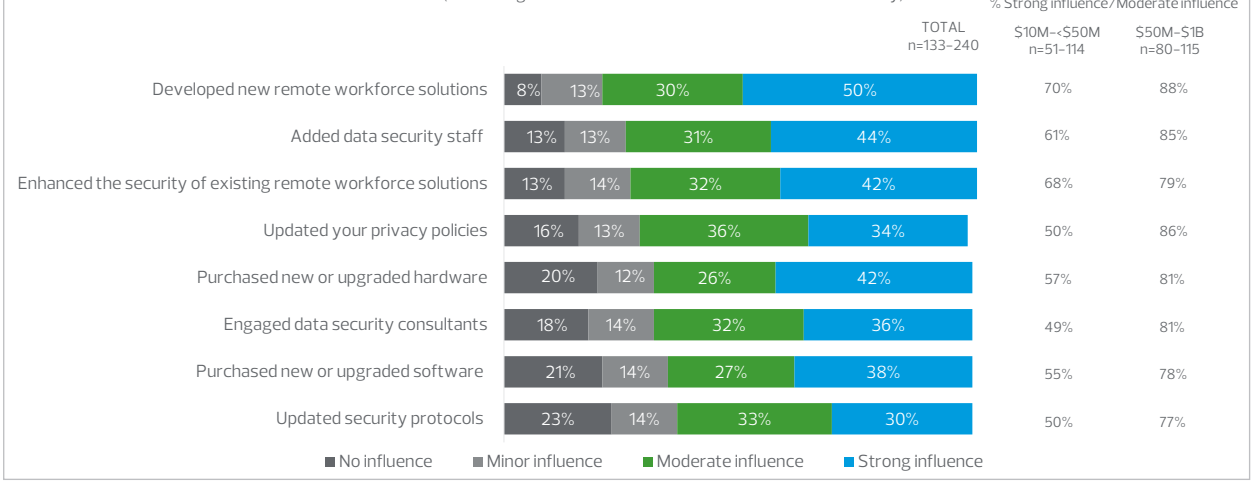
(BASE = had ransomware attack in last year or outside parties attempted to manipulate employees by pretending to be trusted third parties or company executives)



Many middle market companies responded to the challenges of the pandemic environment by making adjustments to their security posture. For instance, among companies in the survey that took actions to enhance their own IT and data security in response to well-publicized breaches, security concerns with COVID-19 were either a moderate or strong influence on 80% of companies that developed new workforce solutions. Comparatively, the pandemic had an influence on 75% of companies that added data security staff and 74% of organizations that enhanced the security of existing remote workforce solutions.

Level of influence that security concerns with Covid-19 had on actions to enhance IT and data security

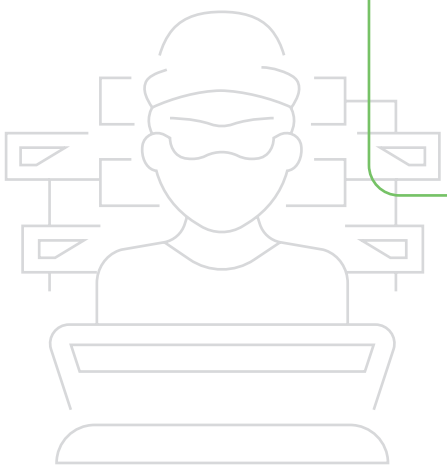
(BASE = organization took actions to enhance IT and data security)



Security concerns with COVID-19 were either a moderate or strong influence on

80%

of companies that developed new workforce solutions



The threat is increasing, but the middle market is responding

The focus on the middle market by cybercriminals is not a new phenomenon—it just may be a way of life moving forward as the threat continues to increase. Middle market companies typically possess valuable data and intellectual property, but lack the level of resources and ability to invest in controls of larger enterprises. However, while cyberattacks will likely never be completely eliminated, middle market companies are showing some indications that they may be moving toward controlling risks better in the future.

The RSM MMBI survey found that 93% of middle market executives claim they are confident in their current measures to safeguard data, down 2% from last year's survey, but still obviously an overwhelming majority. In contrast to that optimism, the highest percentage of respondents in the history of the survey reported a data breach—28% compared to 18% last year and just 5% going back to 2015 when the survey began.

In the past, middle market companies have seemed overconfident in security measures as breaches continued to climb—and that still may be the case to some extent. But middle market companies appear to be making progress in some key areas that may be extremely beneficial in resisting cyberattacks or at least lessening their impact.

71%

of middle market executives indicated that their **organizations had a dedicated function focused on data security and privacy**

For example, 71% of middle market executives indicated that their organizations had a dedicated function focused on data security and privacy. This is actually the same percentage as last year's survey; but overall, 90% of respondents are taking specific actions due to publicized data security breaches—including a record-high 33% of companies adding data security staff. The survey also saw record highs in some protections against specific types of attacks, such as 53% of companies providing training for employees to identify and prevent social engineering attacks.

"We generally see a spike in companies' interest level when a breach occurs within their specific industry, said RSM National Leader of Security and Privacy Services Tauseef Ghazi. "Companies track the overall breach, and focus on the attack vector that led to the compromise to ensure that they are protected and to avoid becoming a 'me too' in the news."

"With the pandemic, investments in disruptive innovation continues to be a trend," commented Ghazi. "Cybersecurity should match these investments to ensure that there is a balance between managing risks while adopting innovative technology to enhance the core business."

In addition, companies taking advantage of cyber insurance in this year's data rose slightly, but more importantly, executives who know the details of their coverages jumped drastically. Policies are not one-size-fits-all, and they are only effective if they provide sufficient coverage for a company's specific risks and vulnerabilities. In this year's survey, 64% of respondents whose firms carry cyber insurance say they are familiar with what their policy covers, up from 48% last year.

64%

of respondents whose firms carry cyber insurance say they are **familiar with what their policy covers**

Many middle market companies also seem to be taking measures to adapt to a quickly evolving data privacy landscape. A record percentage of survey respondents report at least some level of familiarity with the requirements of the GDPR European data privacy standard (55%), and 97% of those executives consider preparing for emerging privacy legislation a priority of at least minor importance.

Finally, a large subset of middle market companies continues to leverage the cloud to increase security. While the 40% of respondents who said they moved or migrated data to the cloud for security concerns was a slight decrease from last year's survey, 54% of those executives who depend on the cloud believe the data they migrated to the cloud is much more secure—a 14 point increase from last year. If this trend continues, we could see even more companies transition key data to the cloud.

The middle market is still under immense pressure from hackers, and that is not likely to change any time soon. But the tide may be slightly turning, as executives make adjustments to staffing, controls and security policies, and begin to see the benefits of those investments. Middle market leaders generally understand that they are not too small for criminals to ignore, but now, keeping pace with security and privacy advancements can go a long way to discouraging and deflecting breach attempts.

54% of executives who depend on the cloud believe the **data migrated to the cloud is much more secure**

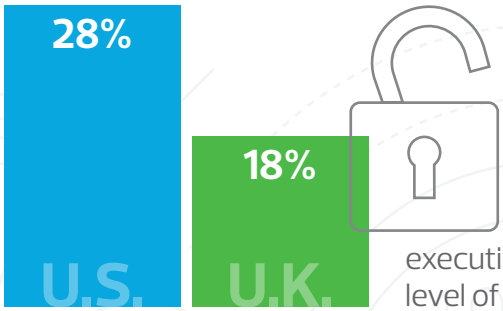
ACROSS THE POND:

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

With geographic boundaries less significant as the economy goes increasingly global, many U.S.–based companies already have business interests in the U.K., or may be considering future expansion into the region. With data from the new RSM U.K. Middle Market Business Index Cybersecurity Special Report, we can now make key comparisons to concerns and protective measures in the United States, and perhaps shed some light on the future of cybersecurity in the United Kingdom.

"The risk of a breach originating from the United States or U.K. can have significant impacts to either entity," commented Ghazi. "Global cybersecurity programs need to take into account all associated cybersecurity attack vectors, and unfortunately, many times that includes overseas operations."

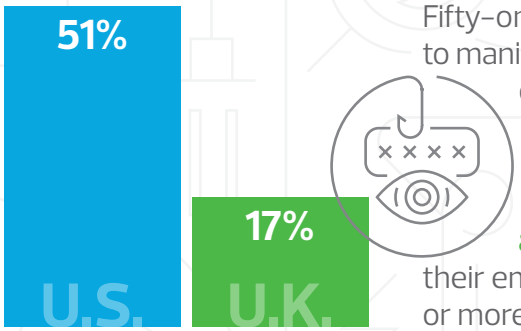
More breaches occurred in the United States, but more executives expect attempts in the U.K.



DATA BREACHES EXPERIENCED

In the United States, 28% of respondents experienced a data breach in the last year, while only 18% of U.K. executives reported one. **However, while 64% of U.S. respondents expect unauthorized users to attempt to access data or systems in 2021, 73% of U.K. counterparts expect a breach attempt.** U.K. executives may fear that they have not yet experienced the level of attacks U.S. companies have faced.

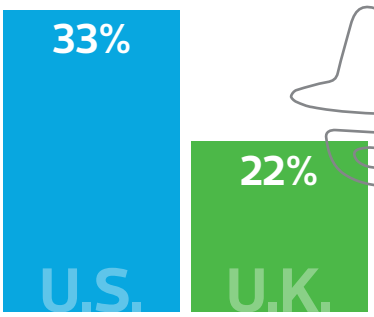
U.S. companies experienced more social engineering attempts, but success was comparable.



SOCIAL ENGINEERING ATTEMPTS

Fifty-one percent of **U.S. respondents** had outside parties attempt to manipulate employees by pretending to be trusted third-parties or company executives, with **45% of those companies ultimately suffering successful attacks**. Only 17% of **U.K. companies** reported a manipulation attempt, but **50% of those organizations ultimately experienced a successful attack**. More U.K. executives provide training, but more of their employees acted on fraudulent requests—so perhaps, more or more targeted training may be necessary.

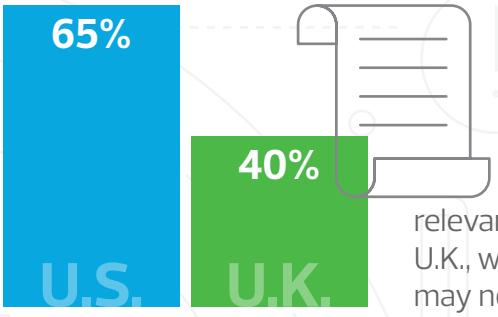
The ransomware threat is more pronounced in the United States—for now.



RANSOMWARE ATTACKS

One and a half times as many middle market executives in the **United States reported a ransomware attack than in the U.K. (33%–22%)**. However, once again, more U.K. companies expect an attack in the coming year (73%–64%). While ransomware attacks have been popular in the United States in recent years, it appears that U.K. executives fear that the tactic has yet to reach its peak across the Atlantic.

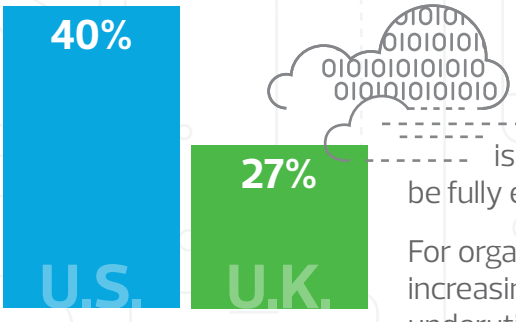
Cyber insurance is more extensively leveraged in the United States.



CYBER INSURANCE

Many more survey respondents carry a cyber insurance policy in the United States than **in the U.K. (65%–40%)**. In fact, among U.K. respondents who do not carry cyber insurance, 59% reported that they did not think it was relevant. Cyber insurance appears to not be as prevalent yet in the U.K., with more restrictive coverages from providers and users that may not have seen the benefits of coverage at this point.

More U.S. middle market companies report leveraging the cloud for data security.



CLOUD FOR DATA SECURITY

In the United States, 40% of survey respondents moved or migrated data to the cloud for security concerns in the past year, **compared to 27% in the U.K.** A similar number of respondents in the two surveys feel their data is more secure in the cloud; so while the strategy may not yet be fully embraced in the U.K., usage will likely grow in time.

For organizations with U.S. and U.K. operations, understanding increasing cyber risks abroad and protections that may be underutilized can help develop a more effective cybersecurity approach, and further protect sensitive data and systems.

Information and data security

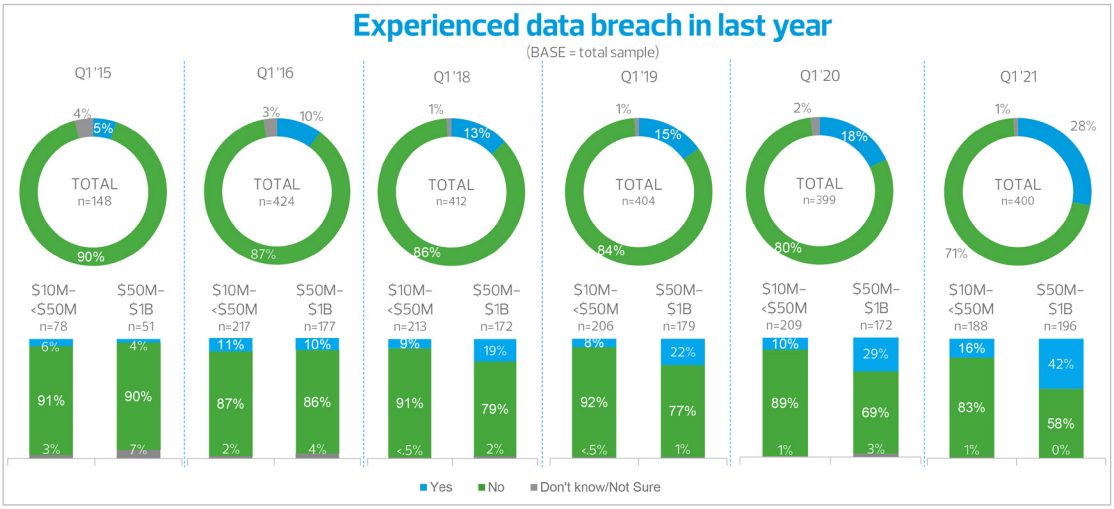
Looking back at 2020, it was a difficult year for middle market organizations for myriad reasons. The COVID-19 pandemic threatened employee safety and overall sustainability, and required significant shifts in established business processes in many cases to maintain productivity. Unfortunately, these new processes added layers of complexity when just trying to keep the business moving, creating a perfect storm for hackers to exploit existing and new vulnerabilities.

From the beginning of the pandemic, cybercriminals launched a web of attacks with varying levels of sophistication intended to prey on users' sense of uncertainty. Hackers only intensified their attacks on middle market businesses when a large segment of companies transitioned to a work-from-home structure, away from more secure internal networks and increasing reliance on the internet. Making that significant and sudden shift was necessary, but it left organizations more susceptible to attacks.

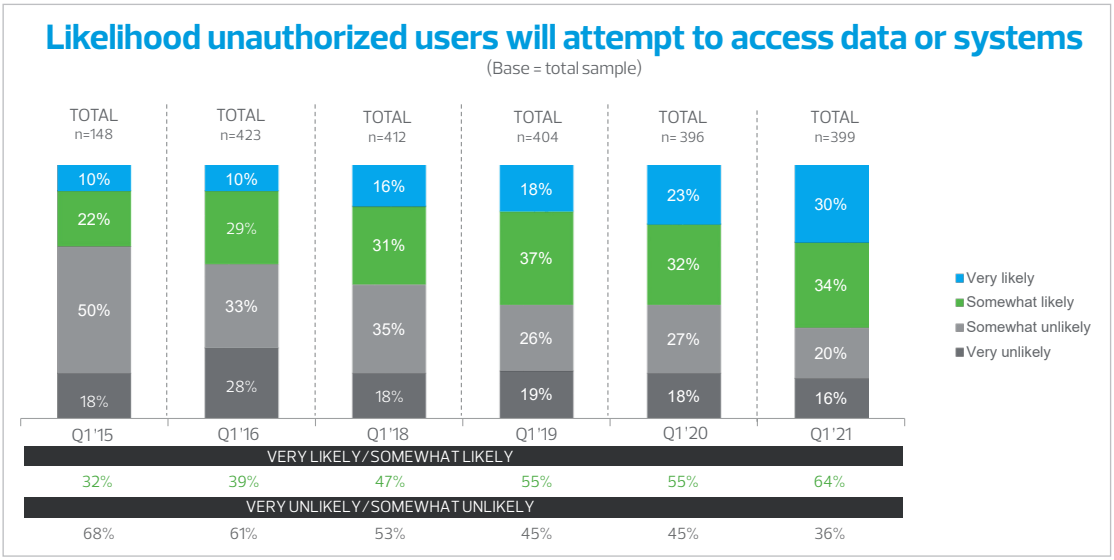
RSM's 2021 first quarter Middle Market Business Index survey gathered data from 400 senior executives at middle market companies about their cybersecurity and data privacy challenges, providing a glimpse into how the largest segment of the U.S. economy is managing threats. In many cases, survey research 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.

The survey shows that the cybersecurity threat is not only growing for middle market companies, but significantly in many areas. For example, the percentage of respondents who experienced a data breach in the last year rose to 28%, the largest year-over-year increase since RSM began tracking this measure in 2015. Last year, 18% of executives disclosed a breach, continuing the annual climb that began with only 5% breached in 2015.

"Data theft issues are increasing day-by-day and causing a lot of problems," said one retail executive. A finance executive agreed: "Our business is having a major issue protecting our business data from all the breaches and thefts."



Given their experience over the last few years, it appears that middle market executives understand the cybersecurity challenges in front of them. In fact, 64% percent of MMBI survey respondents indicate that unauthorized users are likely or very likely to access data or systems this year—again, a new high. That number was stable at 55% over the two previous years before jumping nine percentage points this year.



Many middle market companies are active in their efforts to address cybersecurity threats, as 71% of RSM survey respondents reported having a dedicated function focused on data security and privacy. This number is consistent with last year's survey, and larger middle market companies are slightly more likely to have a focused security and privacy platform, with 75% leveraging the resource compared to 67% of smaller organizations.

"Having a dedicated cybersecurity resource is a key component to ensuring cyber risks stay at the forefront of executives' minds," said Ghazi.

Organizations took a wide variety of actions in response to publicized data security breaches in the past year, and made changes to some existing processes. Most notably, 33% of middle market executives reported they added data security staff, a record high. However, companies that updated security protocols dropped to 60% from 71% in 2020, and those that purchased or upgraded software fell to 46%. These two metrics likely fell due to financial constraints and uncertainty as the COVID-19 pandemic unfolded.

One retail executive provided insight into that exact scenario. "Due to COVID-19, our organization cannot provide new technology for securing company data from fraud and cyberattacks."

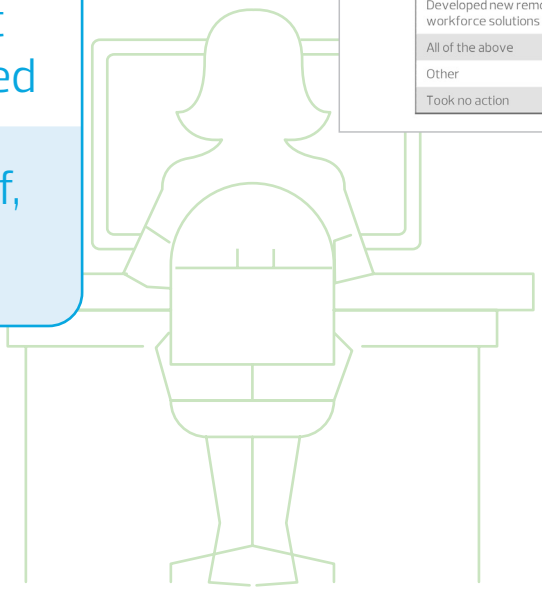
Actions organization has taken due to publicized data-security breaches

(BASE = total sample – multiple responses allowed)

	Q1'21		
	TOTAL n=399	$10M–<$50M n=188	$50M–$1B n=196
	%	%	%
Updated security protocols	60	60	59
Purchased new or upgraded software	46	48	43
Updated our privacy policies	52	45	58
Purchased new or upgraded hardware	48	47	48
Engaged data security consultants	40	36	46
Added data security staff	33	27	41
Enhanced the security of existing remote workforce solutions	55	57	53
Developed new remote workforce solutions	46	41	49
All of the above	6	7	5
Other	2	3	1
Took no action	10	14	6

33%

of middle market executives reported they added data security staff, a record high



Ghazi sees the importance of staffing increases at middle market companies, especially as some companies reduce funding in other areas. "While our research shows more companies are hiring security staff, this may also explain the drop in updating security protocols and upgrading software. It's not surprising to realize that many organizations have invested in cybersecurity software and components; however, many haven't fully utilized or implemented these technologies. By having a dedicated cybersecurity resource on staff, it allows organizations to efficiently use the existing technology, versus buying new software that potentially sits on the shelf."

Middle market organizations had a lot to contend with in 2020—unprecedented changes were necessary to business processes as companies adapted to a pandemic environment, and cybercriminals were quick to strike with a record-high level of success. However, it's clear that middle market organizations have been making strategic changes to keep up with new risks, and that focus will need to continue and sharpen moving forward to address threats that are certain to continue evolving over time.

Cyber insurance

With the number of breach attempts and successful breaches surging, cyber insurance has never been more valuable to middle market companies. A well-defined and properly scoped policy can help organizations better protect critical data and systems and provide the necessary support to quickly recover from a potential breach.

Cyber insurance has steadily grown to become a key pillar of an effective cybersecurity approach. Even in recent years, many companies may not have necessarily been completely familiar with how policies work or what coverages were available. However, we are now seeing some signals that the middle market is better embracing cyber insurance as a key protective measure.

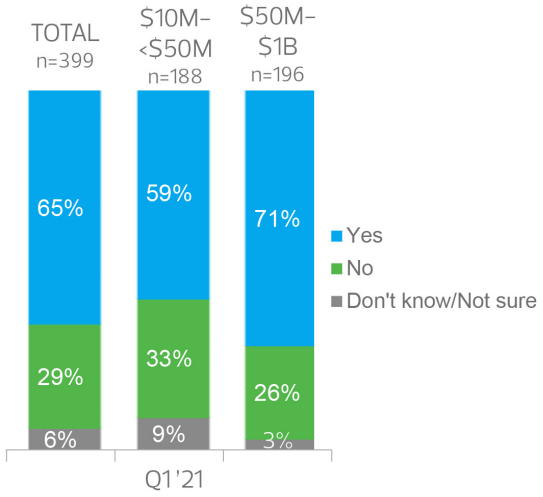
The RSM MMBI survey found that 65% of respondents currently use a cyber insurance policy to protect against internet-based risks. That number has steadily risen each year, and represents a 3% increase from last year's data. Similar increases were seen in the data for larger middle market organizations that carried a cyber insurance policy (71%), as well as their smaller counterparts (59%).

Awareness of coverages for larger middle market companies rose to

80%

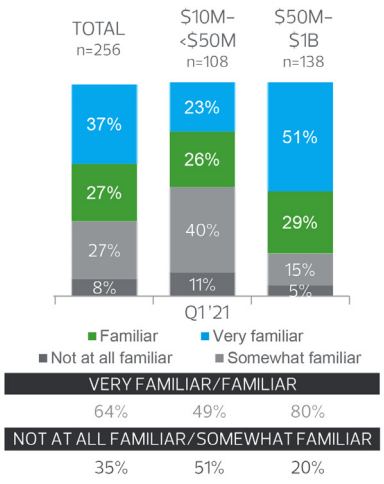
Organization carries a cyber insurance policy

(BASE = total sample)



Familiarity with what organization's cyber insurance policy covers

(BASE: carries cyber insurance)



A cyber insurance policy is meant to be a supplement to traditional liability insurance, which typically does not offer coverage for cybersecurity incidents. Companies must know where any coverage gaps exist and how the two policies interact to ensure that the desired level of protection is met. Just like with a traditional insurance policy, middle market organizations do not want to assume an area is covered and then find out otherwise after an attack.

However, in addition to the steady rise in coverage overall, the survey found that more middle market executives know what their specific coverages are. Among middle market organizations that carry cyber insurance policies, 64% of executives reported that they are familiar with their policy coverage, a sharp increase from 48% last year. Awareness of coverages for larger middle market companies rose to 80%, while smaller companies saw an increase to 49%.

A cyber insurance policy is only as good as the details of the protections it offers, and the increased awareness of coverages is a positive sign. Providers frequently make changes to coverage limits and options, and middle market organizations must continue to work with their vendor and make adjustments as needed to ensure proper coverages are met.

"When evaluating your cyber insurance policy, make sure to align it to your cyber risks, and use the insurance policy as a platform to protect against catastrophic events," said RSM National Leader of Cyber Testing and Response Ken Stasiak.

Risks or exposures the cyber insurance policy covers

(BASE: familiar with cyber-insurance policy coverage – multiple responses allowed)

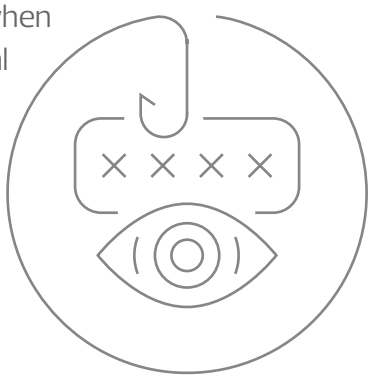
	Q1'20			Q1'21		
	TOTAL n=120	$10M-<$50M n=41	$50M-$1B n=74	TOTAL n=166	$10M-<$50M n=52	$50M-$1B n=111
	%	%	%	%	%	%
Data destruction	74	88	66	68	73	66
Hacking	65	76	59	66	75	63
Business interruption	67	77	60	57	69	50
Denial of service attacks	45	65	34	55	56	54
Failure to safeguard data	51	65	43	53	53	52
Theft	56	79	43	53	57	50
Post-incident investigative expenses	52	60	47	49	54	46
Extortion (including ransomware attacks)	65	82	56	47	66	39
Post-incident public relations expenses	44	52	39	46	51	44
Defamation	31	41	26	39	45	36
None of the above	<.5	0	1	1	0	1

Cyber insurance policies are designed to be very broad and modular, with several potential options available to meet an organization's specific needs. In RSM's survey, middle market executives report that their cyber insurance policies most often carry coverage for data destruction (68%) and hacking (66%). Coverages for denial of service attacks (55%) and defamation (39%) saw sizable increases, while protection for failure to safeguard data (53%) and post-incident public relations expenses (46%) saw smaller gains.

To Stasiak, the increases in cyber insurance coverages have been noticeable. "Over the past year, we have seen an uptick in companies increasing their cyber insurance coverage amounts," he said. "In many cases, limits have been increased substantially."

Of note though, coverages for business interruption (57%) and extortion (47%)—which include ransomware attacks—showed considerable declines over last year.

In the current threat environment, cyber insurance is an imperative protective measure for middle market companies. The financial, reputational and regulatory impact that breaches often create can be extremely harmful, and a well-designed cyber insurance policy can help lessen those damages. However, as with any insurance product, companies must be careful when establishing or renewing a cyber insurance policy to ensure that critical systems and data are protected as intended.



Ransomware attacks

Ransomware has been a growing threat to the middle market in recent years, and that proved to be true once again in 2020. It represents a low-risk, high-reward opportunity for hackers, with little effort often leading to bounties up to millions of dollars to release files. Ransomware attacks can be extremely expensive for middle market organizations to address and often cause productivity to grind to a halt. Therefore, companies must understand how to identify and contain potential attacks before they launch.

Ransomware attacks typically take multiple forms, requiring employees to have a heightened sense of awareness to protect sensitive data and company information. The most common ransomware attack involves criminals repetitively sending fraudulent messages from fake or compromised email addresses designed to be legitimate information. Another common tactic is more sophisticated, specifically targeting networks or systems that have been identified as vulnerable.

Unfortunately, many networks were particularly vulnerable as the COVID-19 pandemic unfolded, especially as organizations transitioned to a work-from-home environment. Without the traditional security controls in place from on-premise infrastructure and a general feeling of uncertainty, users were more likely to click on questionable links and infect company networks.

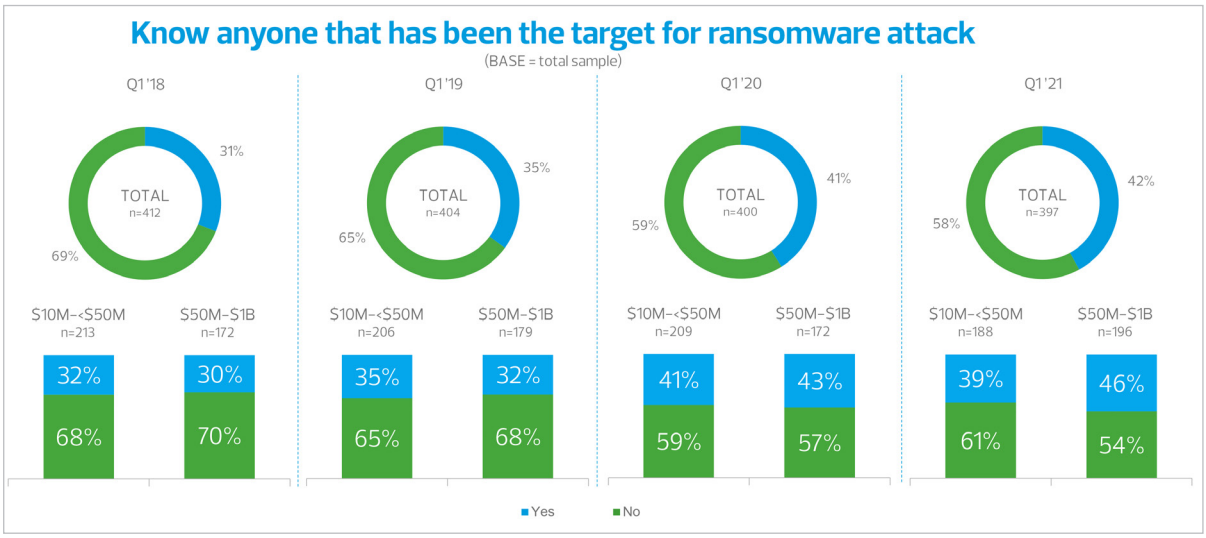
"The pandemic created an opportunistic landscape for attackers seeking to infect organizations with ransomware," said Stasiak.

Once cybercriminals gain access to a network,

they will attempt to restrict access to certain information, or entire segments of a network. A message is then sent from the hacker with details about the locked files or areas, and the specific ransom demands to unlock files 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 can be costly.

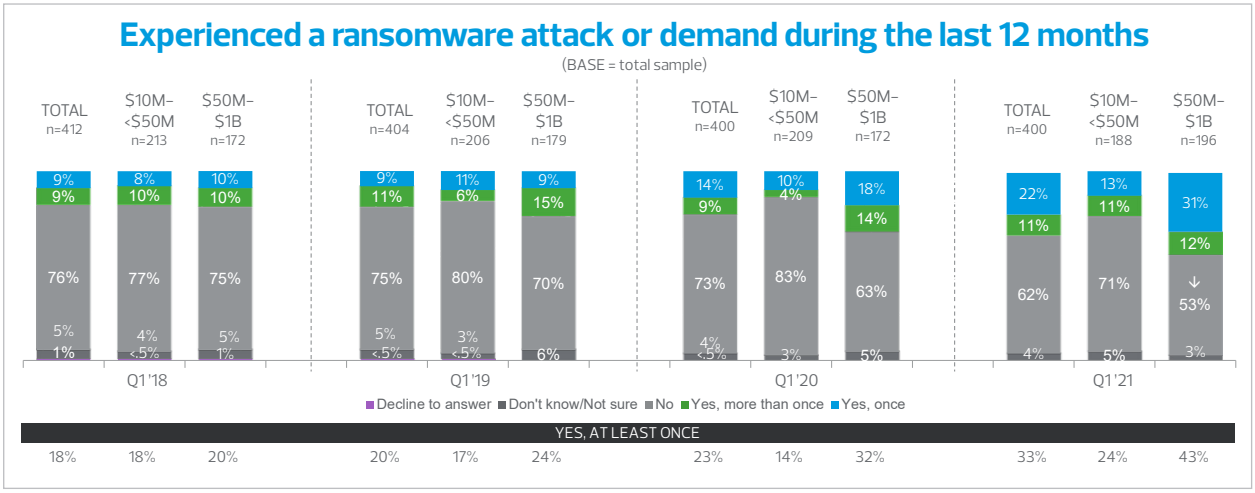
One key reason behind the growth of ransomware attacks is the flood of stolen data to underground markets and the subsequent drop in value for those assets. Instead of the traditional hacking route of attempting to procure and then sell stolen data, many cybercriminals are instead opting for ransomware attacks that are less labor-intensive and provide a more direct route to a more lucrative payday.

Considering the ransomware environment, it's no surprise that more middle market companies said they know a peer that has suffered an attack, or have been a target themselves. The RSM MMBI survey found that 42% of middle market executives know of a company that has been a target of a ransomware attack, a slight increase over last year's data.



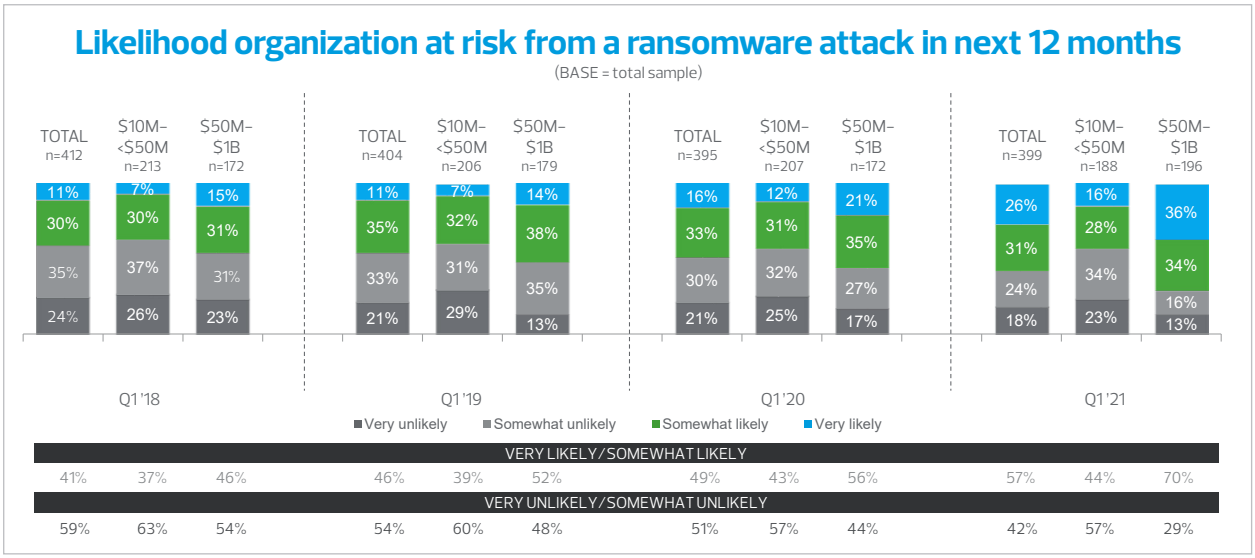
Thirty-three percent of survey respondents disclosed that they experienced a ransomware attack or demand in the last year, the highest number since ransomware became a focus four years ago, and a 10% increase from last year. In addition, 43% of larger middle market organizations reported an attack, compared to 24% at smaller companies.

Compounding the issues related to a ransomware attack, 11% of executive experienced more than one attack in 2020. This is a common tactic by cybercriminals—once a breach occurs, they will continue to attempt to attack the company until it proves that its network is secure.

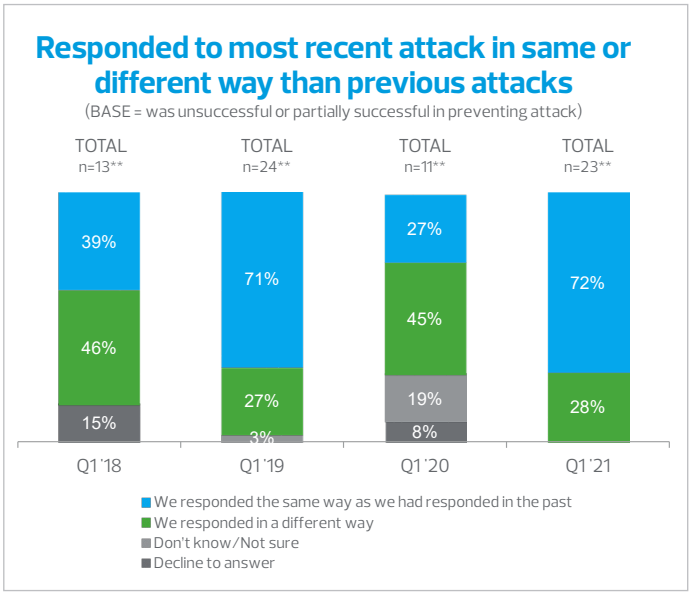


In addition to repeated attacks, Stasiak is also seeing a new threat to middle market companies. "While traditional-style ransomware attacks are still very much prevalent, new variant-style ransomware attacks continue to surface," he said. "These are creating a consistent strain on cybersecurity teams."

Between coverage in the media, attacks on peers and their own experiences, middle market executives appear very aware of ransomware risks. Fifty-seven percent of respondents in the RSM survey said their organizations are likely targets for ransomware attacks this year, an 8% increase from last year's report. Many more executives at larger organizations said the threat was very likely or somewhat likely than at smaller organizations (70% versus 44%).



With the increase in ransomware attacks and more projected for the future, middle market companies may need to reconsider how they respond to attacks. However, 72% of survey participants responded to their most recent attack in the same way as past attacks, compared to just 27% in 2020.



The ransomware threat to the middle market is very real and shows no sign of slowing down. Its combination of ease of deployment and potential high rewards means that all organizations are potentially at risk. With work environments continuing to undergo changes in the midst of the pandemic, companies have an opportunity to evaluate their overall security framework to combat ransomware, introducing new awareness training and incident response planning, as well as strengthening programs for patch management and backups.

72%

responded **to their most recent ransomware attack** in the same way as past attacks

Business takeover threats

Unlike many sophisticated and high-tech cyberattacks, many business takeover attacks fly under the radar due to their low-tech design. Regardless, these attacks can cause a significant amount of damage, and are more harmful because they can be carried out by almost anyone. Common methods include social engineering and employee manipulation attacks—very simple breaches on the surface, but very difficult to steer clear of.

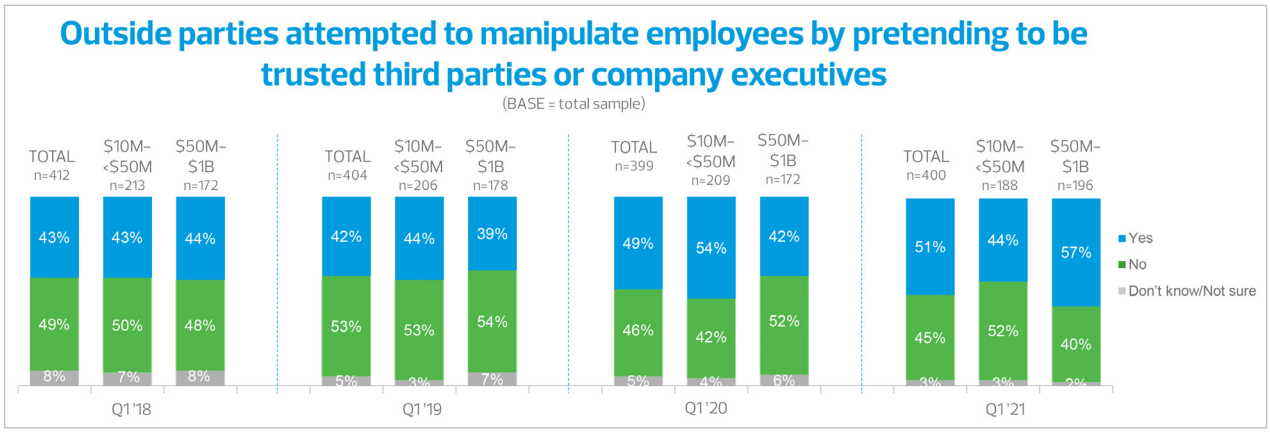
Social engineering has become a favorite attack method among cybercriminals, mainly due to the low level of expertise necessary. An attack can begin by reaching out to an employee—by phone, email or even in person—and attempting to convince them to provide sensitive data or access to that data. The employee is usually tricked because the hacker poses as a co-worker or trusted third party. While these attacks appear simple to carry out, many of these takeover criminals are very skilled in finding and exploiting any potential lack of security awareness.

The most common business takeover strategy is phishing. Hackers gather data from social media profiles or even publicly available company websites to create emails that look like they are from a friend or co-worker. These emails attempt to convince recipients to click on a corrupt link or attachment.

Another proven strategy—fraudulent emails—returned with a vengeance in the early days of the COVID-19 pandemic and continues today. These tactics became commonplace in an attempt to capitalize on fear and panic, promising information on virus spread, protective measures or ways to help charitable or relief organizations. Today, those messages continue, trying to entice readers with vaccination or economic stimulus information.

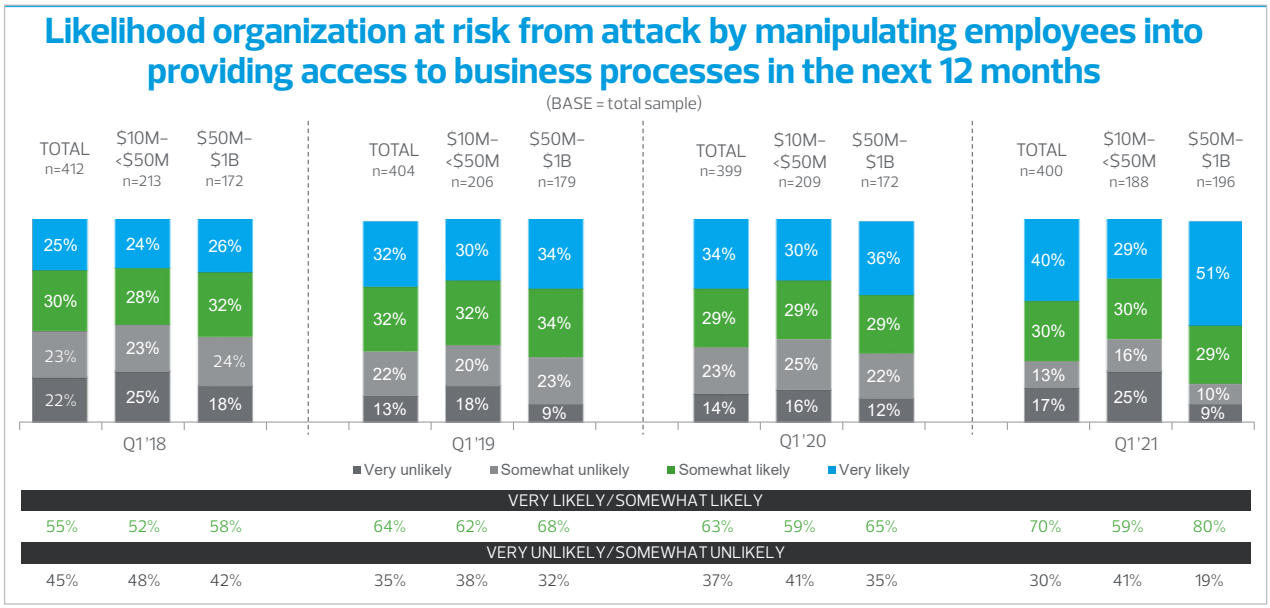
The steady increase in social engineering attacks was evident in the RSM MMBI research, as 51% of middle market executives said that outside parties attempted to manipulate employees by pretending to be trusted third parties or company executives. This represents a 2% increase over last year's data.

In addition, respondents from larger companies reported more of these attacks than those from smaller organizations, 57% versus 44% respectively. This data represents the inverse of 2020's survey information.

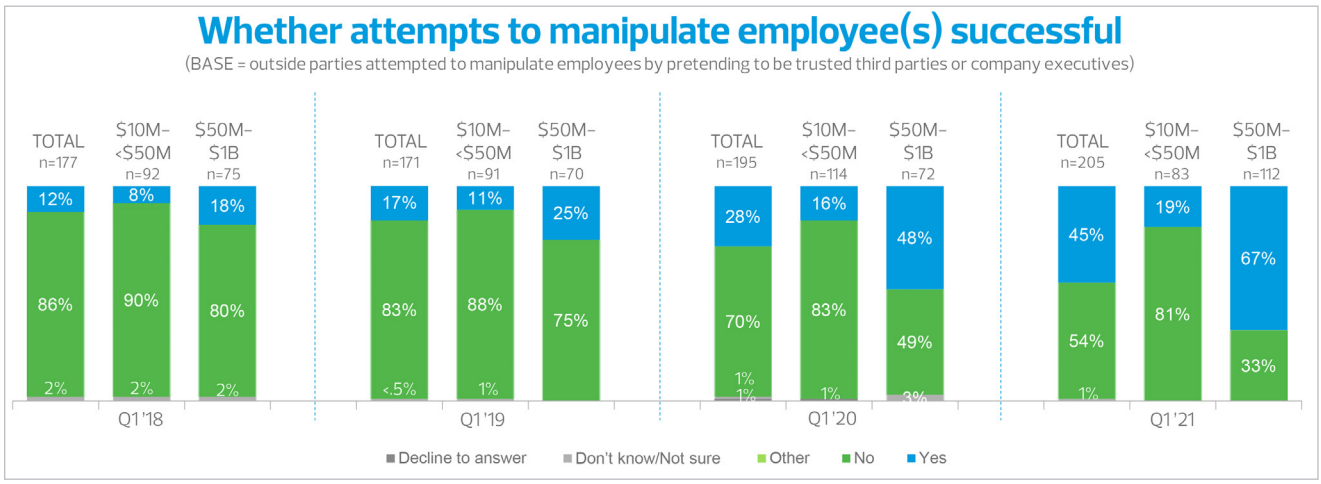


"With social engineering attacks, the more the merrier, and we see that play out with larger middle market companies," commented Stasiak. "By casting a wider net, attackers only need to catch one employee."

The highest percentage of respondents in survey history see the social engineering threat growing this year. In the study, 70% of executives said their organization is at risk of an attack by manipulating employees in the next 12 months, an increase of 7% from last year. The number of smaller organizations expecting an attack stayed consistent between 2021 and last year (59%), but 80% of executives from larger companies said they believed a breach is likely, up from 65% last year.



Unfortunately, many executives may expect more attempts in 2021 because more attacks were successful in 2020. In the survey, executives reported that 45% of social engineering attacks were successful last year, a spike from 28% in the previous year. Attempts were much more successful at larger companies, with 67% of respondents from these companies reporting that manipulation attempts worked, compared to 19% at smaller organizations.



"With an increased attack surface, larger middle market companies continue to see an increase in successful attacks year-over-year," said Stasiak. "While these companies bring more cybersecurity resources to bear than smaller middle market companies, attackers are willing to invest in more targeted attacks given the bigger potential payout from larger companies."

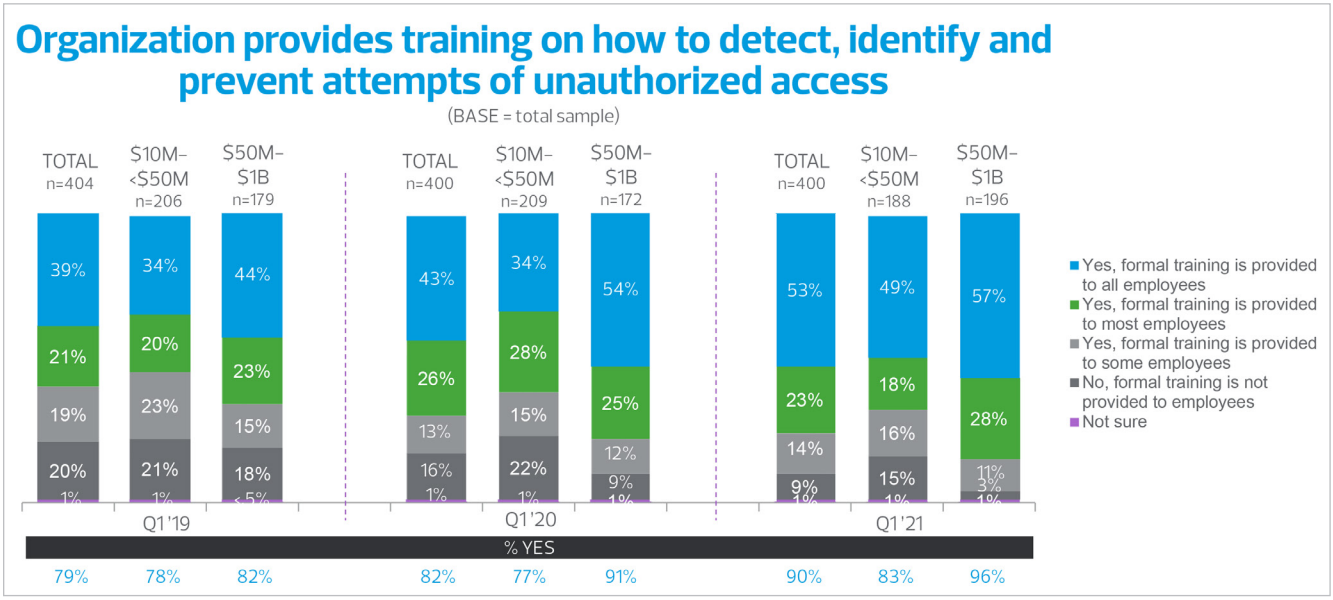
With the broad nature of social engineering attacks, middle market companies need to utilize several strategies to combat them. Of the organizations in RSM's survey that had unsuccessful attacks, 88% listed employees not acting on the fraudulent request as a reason for the failed breach, a 2% drop from last year's survey. Further, 63% of middle market executives said that secondary controls prevented the completion of an attack, and 51% acknowledged system controls that prevented delivery of fraudulent communications or materials to employees.

45% **of social engineering attacks** were successful last year

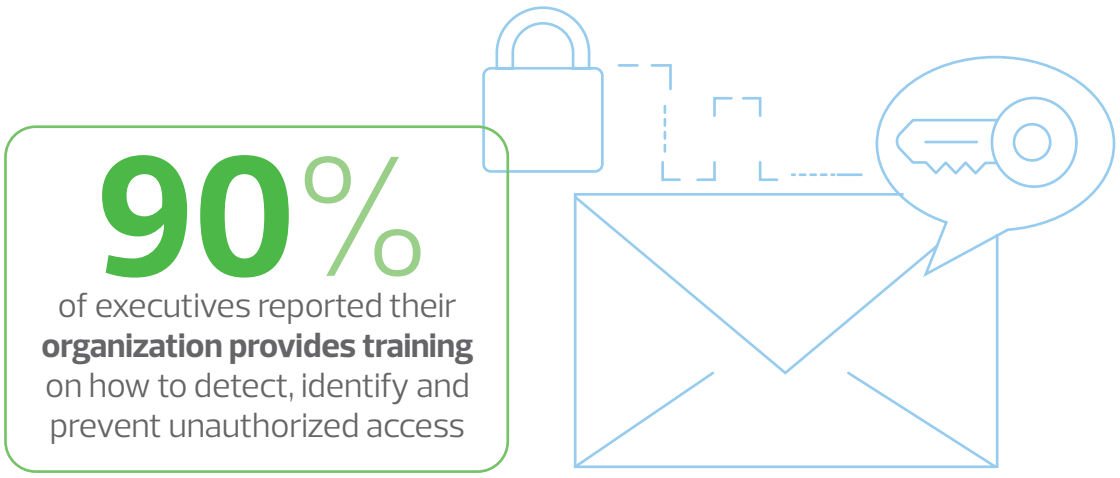
88% listed **employees not acting on fraudulent requests** as a reason for failed breaches

Training is recognized as the best defense against social engineering attacks, providing situational awareness through real-life demonstrations. The majority of survey respondents said they see the value in training, as 90% of executives reported their organization provides training to at least some employees on how to detect, identify and prevent attempts to gain unauthorized access. This represents an 8% increase over 2020's data.

One manufacturing executive detailed how they utilize training to address social engineering risks: "We develop training programs that make our employees aware of attempts to steal data or gain access to our systems."



Stasiak further emphasized the importance of training to an effective security posture. "Social engineering training continues to be the cornerstone of a cyber-awareness program," he said. "Continued investments and testing will ensure that the overall framework continues to be effective against emerging threats."



Privacy protections compliance

While cybersecurity is an ongoing challenge for the middle market, data privacy will also require an increasing amount of attention and focus in coming years. Like all companies, middle market organizations collect a significant amount of data to guide processes and help make business decisions. However, data privacy laws from overseas and within individual states return more power to the consumer and focus on why organizations have some data rather than how it is secured.

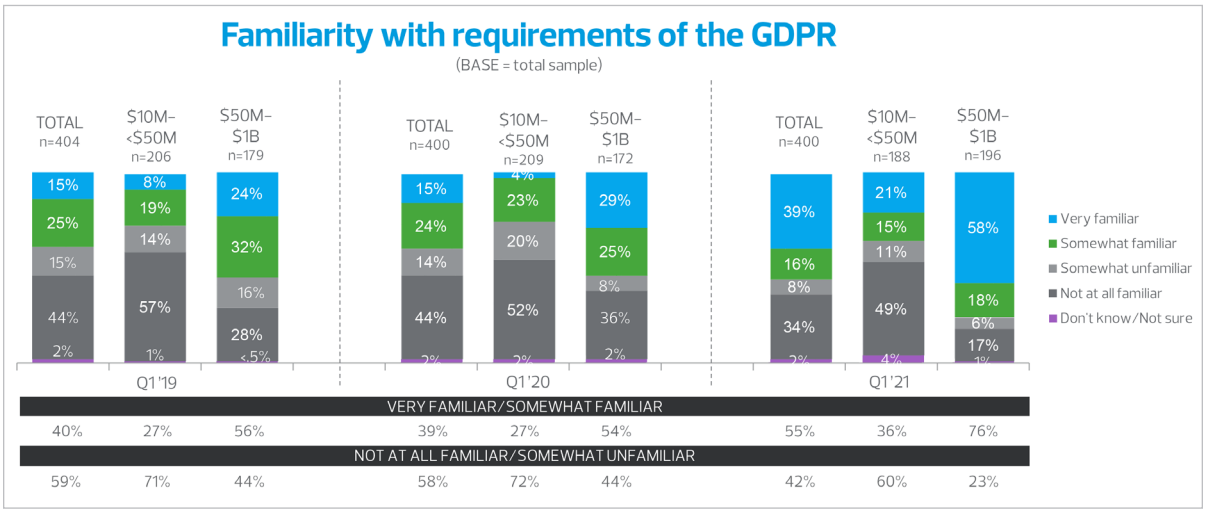
The European Union's groundbreaking General Data Protection Regulation was implemented in 2018 and has since served as a model for data privacy legislation around the world. The GDPR set a standard for how companies transmit, process or hold EU resident data, regardless of whether a company actually has European operations. Many companies outside of Europe were slow to implement GDPR-compliant processes, but following many high-profile enforcement actions, effective compliance programs became more commonplace.

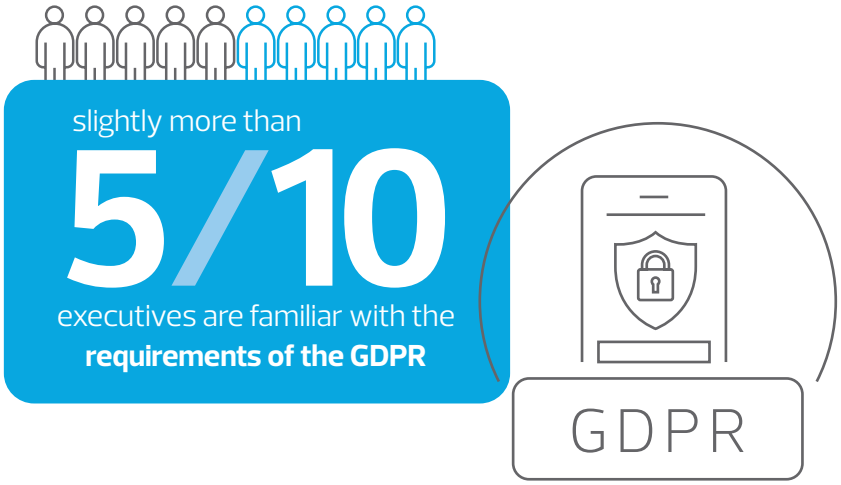
Following the initial success of the GDPR, plans for data privacy legislation began formulating in the United States. Since the GDPR took effect, the United States has seen over a dozen individual state data privacy laws go into effect, including the well-publicized California Consumer Privacy Act.

For many years, a federal data privacy standard has been considered in the United States by both Democrats and Republicans. In recent years, it has seemed like a "not if, but when" proposal: and now, under the current administration, it may be closer than ever before. During the 2020 election, data privacy was an element of both parties' platforms, but it was more of a priority from a Democratic Party perspective. Following the election of President Joe Biden, data privacy is likely to come to the forefront sooner rather than later.

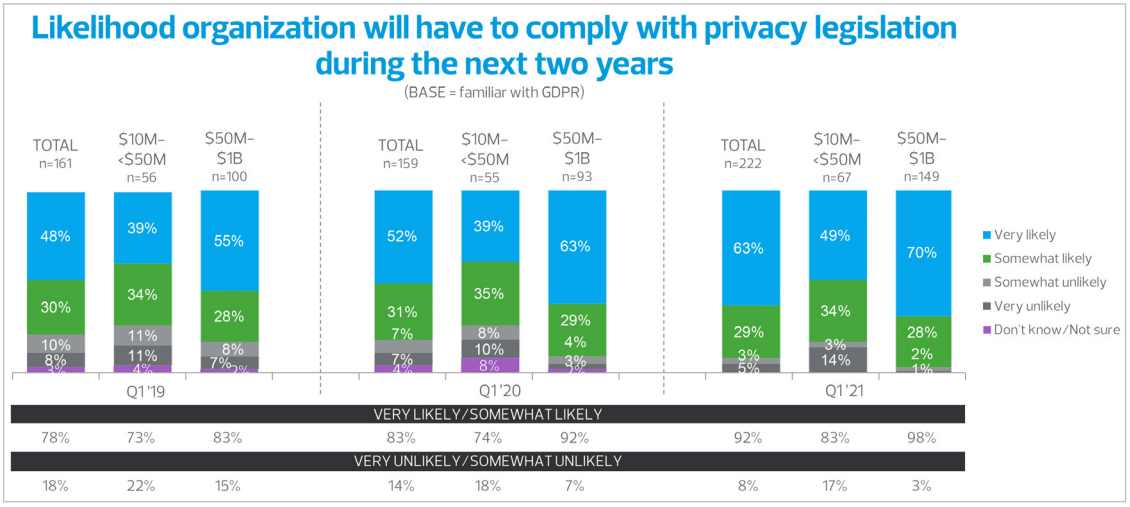
"While the United States still lags behind many countries when it comes to data privacy, we have seen a significant increase in overall awareness along with new state and federal regulations to protect consumer data," said Ghazi.

Many middle market companies are subject to GDPR regulations, and awareness of the standard is growing. Fifty-five percent of executives in the RSM MMBI survey said they are familiar with the requirements of the law, a 14% increase from last year's data. Respondents from larger organizations were more familiar with GDPR requirements than those at smaller organizations—76% versus 36%.

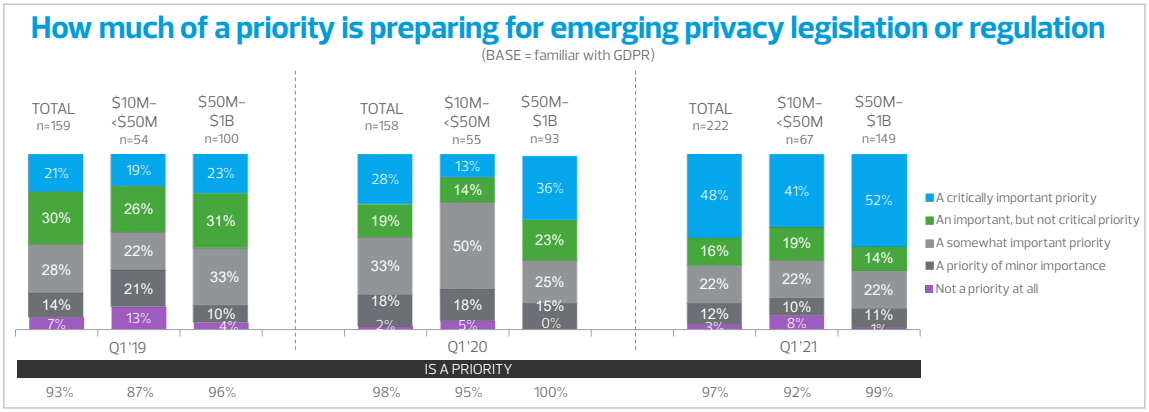




With data privacy becoming more of a focus in the United States, many middle market companies understand they will likely need to adhere to new laws in the near future. Among RSM survey respondents familiar with GDPR regulations, 92% said that their organizations will likely have to comply with privacy legislation similar to the GDPR at a state or federal level in the United States during the next two years, a 9% increase from the 2020 survey.



Given the strength of the GDPR and many of the existing U.S. data privacy regulations, it appears that middle market executives are taking current and future legislation seriously. For example, 97% of executives in the RSM survey who are familiar with the GDPR said preparing for emerging privacy regulations is a priority, a nominal drop from last year's data. Ninety-two percent of smaller middle market organizations are prioritizing data privacy preparations, compared to 99% of larger companies.



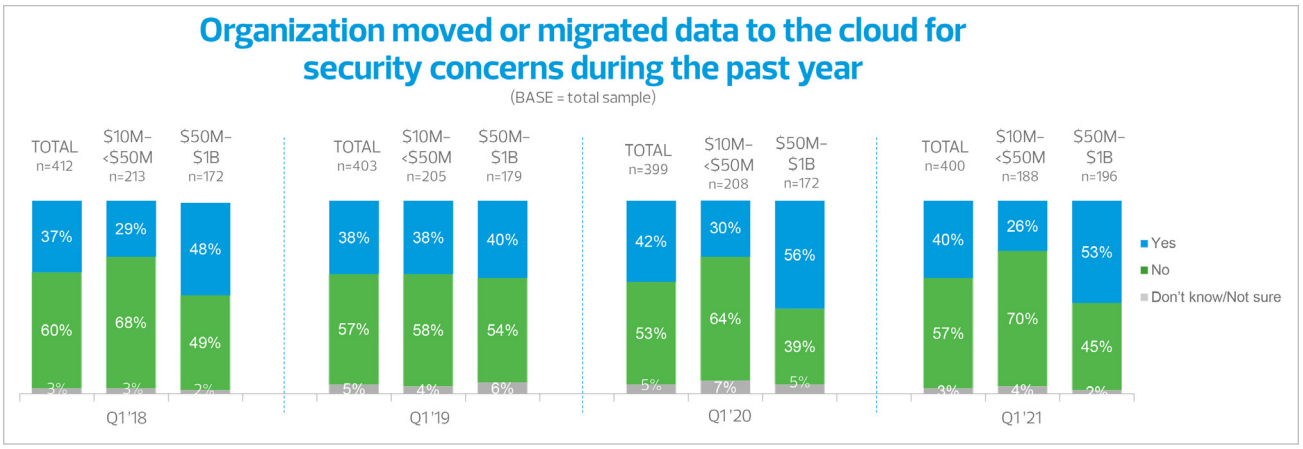
For many years, data privacy legislation was seen as the future of security and privacy—but with recent advancements, the future is now. Momentum is quickly moving toward additional data privacy regulations from a federal and state perspective, and middle market companies should prepare to comply with legislation in the near future. Companies can ready themselves for potential upcoming standards by comparing existing processes to data privacy laws that are currently in effect. Many have common elements, and new state or federal legislation will likely include several familiar hallmarks.

Migration to the cloud to ensure data security

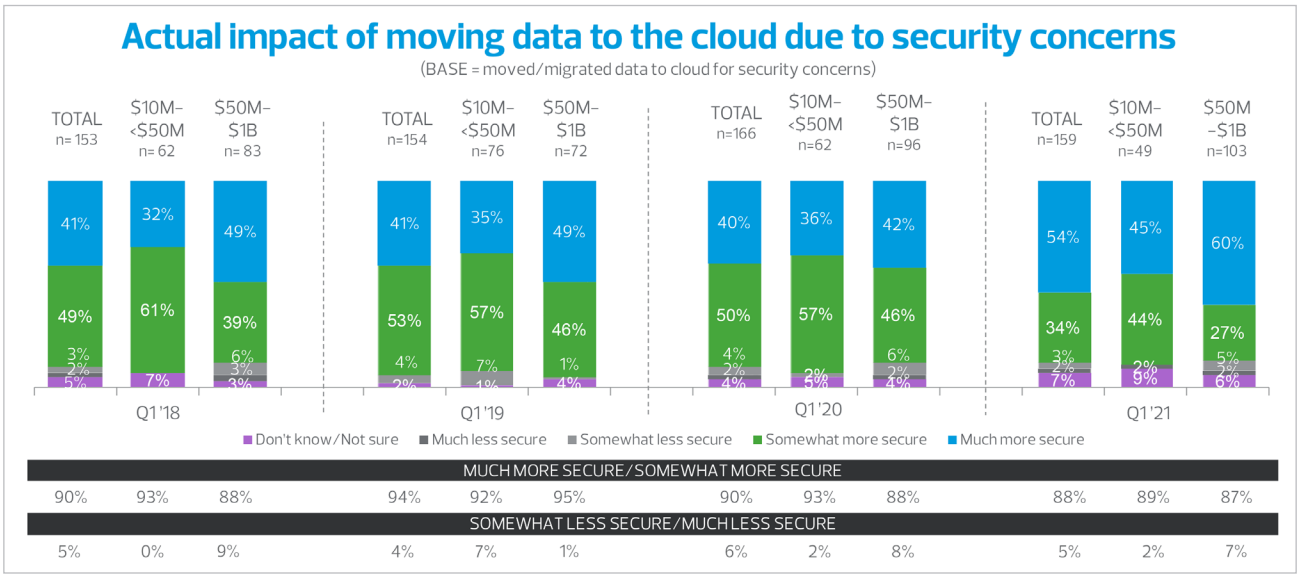
The cloud has been an extremely valuable tool for middle market organizations; and at this point, almost every company leverages the cloud in some manner. Many companies use the cloud to gain control over data or increase access and visibility into information, but it is also gaining traction as a security tool. With the increasing scale of many cloud providers, they can deliver security capabilities that may be out of reach for middle market companies coupled with storage options that can typically meet a variety of business needs.

"Cloud providers continue to evolve with new features and benefits, which may entice many companies to move to a full-cloud or a hybrid environment," said Stasiak.

The RSM MMBI data shows that a fairly consistent number of middle market executives are utilizing the cloud to increase data security. In fact, 40% of survey respondents detailed moving or migrating data to the cloud for security concerns in the past year, a 2% reduction from the previous year's data. More than twice as many larger middle market organizations are moving to the cloud because of security than smaller organizations—53% compared to 26%.

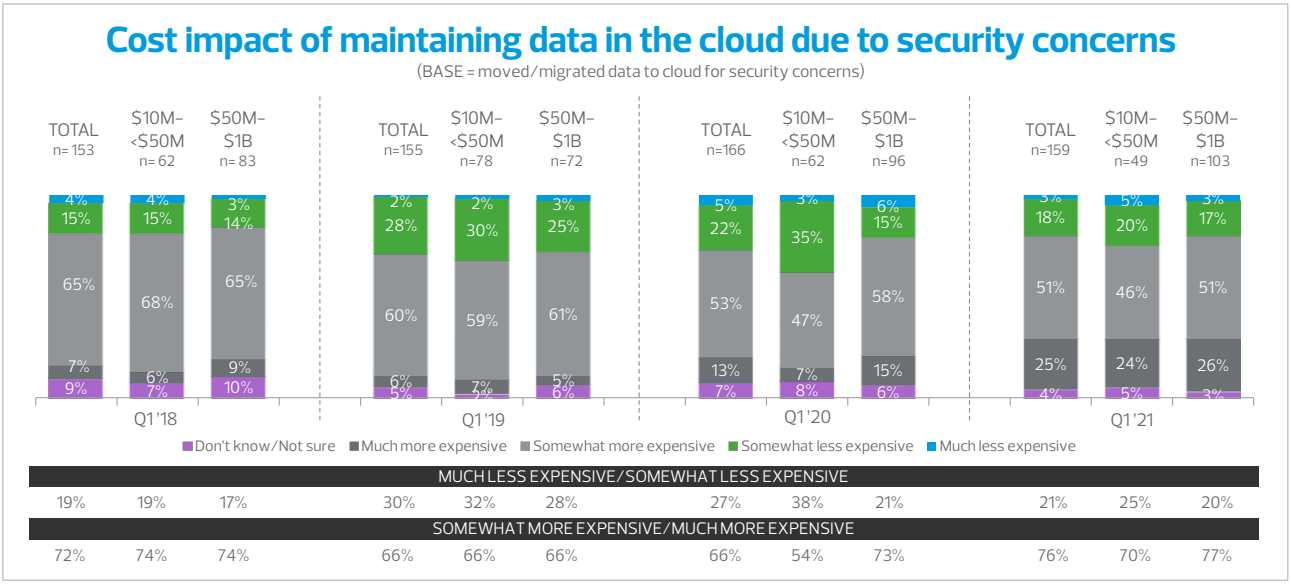


While middle market movement to the cloud for enhanced security may have stalled slightly, the overwhelming majority of companies that are utilizing the cloud are certainly seeing results. Among middle market executives reporting moving data to the cloud for security concerns, 88% believe the data residing in the cloud is more secure. This actually represents a 2% drop from last year's survey, but 54% feel that their data in the cloud is much more secure, the highest level in survey history.



While respondents seem largely satisfied with the level of security in the cloud, Stasiak cautions that hackers are paying increased attention to the cloud service providers. "Over the past couple of years, we have seen a significant increase in cloud-related attacks and custom-developed exploits," he said. "I don't think this trend is going to slow down, especially as more and more companies move critical applications to the cloud."

The cloud can provide cost savings in some applications, but reaching a higher level of security often comes with an increased expense. The RSM survey finds that 21% of middle market executives said the cost of maintaining data in the cloud was less expensive, a 6% decrease from last year's data. On the other hand, 76% of respondents considered storing data in the cloud for security reasons more expensive.



While the cloud may not be for everyone, it should at least be evaluated as a potential protective measure for sensitive data. In almost all cases, the cloud provides better access, organization and security for data, but cost can become an issue. However, some of those cost pressures may be alleviated through a due diligence process that evaluates multiple providers to best match expectations with capabilities.

21%

of middle market executives said the cost of maintaining data in the cloud was less expensive

Methodology

About the RSM US Middle Market Business Index research

The RSM US Middle Market Business Index survey data in the first quarter of 2021 was gleaned from a panel of 700 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 2020 first quarter survey was conducted from Jan. 11 to Jan. 29, 2021. Information was collected by phone and online survey from 400 executives, including 233 panel members and a sample of 167 online respondents. Data is weighted by industry.

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

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

For media inquiries, please contact Terri Andrews, national public relations director, +1 980 233 4710 or terri.andrews@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

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.

U.S. CHAMBER OF COMMERCE