RSM US MIDDLE MARKET BUSINESS INDEX

CYBERSECURITY

SPECIAL REPORT

U.S. CHAMBER OF COMMERCE

RSM

RSM US MIDDLE MARKET BUSINESS INDEX

CYBERSECURITY

SPECIAL REPORT

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

TABLE OF **CONTENTS**

EXECUTIVE SUMMARY

THE MIDDLE MARKET HAS BECOME GROUND ZERO FOR THE CYBERSECURITY THREAT

MIDDLE MARKET COMPANIES have increasingly become the primary target for cybercriminals, with data security incidents rising incrementally each year. Attackers typically know that large organizations have invested heavily in security, so the success rate does not often justify the effort. However, the middle market is big enough to yield significant results for hackers without having to contend with the mature controls of their larger rivals.

In addition, the COVID-19 pandemic has increased the complexity of cybersecurity challenges for the middle market. As the new distributed workforce has become even more dependent on the internet to remain productive, hackers are taking advantage of the crisis by unleashing a variety of attacks that larger organizations are often better equipped to address. And, in an unprecedented public health situation, where organizations must focus on employee safety and keeping the business running, cybersecurity processes require heightened attention.

Generally, middle market companies understand the threats that hackers present; but unfortunately, cybercriminals are often ahead of the latest protections and their methods can evolve quickly. Middle market executives recently detailed the increase in data breaches in the sector in a recent RSM US Middle Market Business Index survey, while also outlining their ongoing cybersecurity concerns and strategies for addressing security gaps.

According to first quarter 2020 MMBI data, 18% of middle market C-suite executives claimed that their company experienced a data breach in the last year, up from 15% in 2019 and continuing the steady rise over the last six years. Larger middle market companies appear to be the most at risk, with executives reporting nearly three times the incidents of smaller midmarket peers.

Despite increased investments in security and the implementation of policies geared toward training, the cybersecurity threat continues to rise. In fact, for the second straight year, RSM's survey found that more than half of middle market executives surveyed indicated that there will likely be an attempt to illegally access their organizations' data in 2020.

This data only emphasizes the importance of cyber insurance. The RSM survey finds that the number of middle market companies that carry policies has indeed risen in the last year. However, less than half of middle market executives with policies are familiar with their policy coverages.

"Cybersecurity is as much an enterprise issue as it is a technical issue; senior company leaders need to work closely with their information security teams to understand the threats applied to their networks, the risks posed by malicious actors, and the risks of inaction. Advanced persistent threats require advanced and persistent countermeasures, both sophisticated and simple. In addition, cyber insurance will become an increasingly important tool in managing cyber risk, but it must be used in conjunction with—and not in lieu of—mature cybersecurity practices."

—Christopher D. Roberti, Senior Vice President for Cyber, Intelligence and Supply Chain Security Policy, U.S. Chamber of Commerce

Beyond increasing threats of cyberattacks, the regulatory landscape continues to shift, providing higher levels of consumer protection in the United States and abroad. The European Union's General Data Protection Regulation was implemented in 2018, governing how EU residents' personal information is collected and stored. Domestically, similar individual state regulations quickly followed suit, with a Nevada law taking effect in October 2019 and California regulations becoming effective at the beginning of this year. Additional state laws will take effect this year.

The legislation has specific state variations, but it is designed to more strictly regulate how companies possess and manage consumer data. Unlike past regulations, these laws are not focused on how companies are protecting data, but rather why they have the data in the first place. Middle market companies are highly reliant on customer information to make business decisions, and the new laws will likely result in significant process changes.

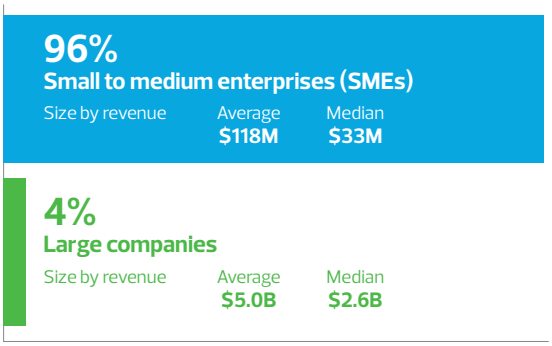
In the RSM MMBI survey, the number of executives who are familiar with GDPR requirements slightly dropped compared to last year. However, nearly all respondents familiar with the GDPR indicated that preparing for emerging privacy legislation is at least a priority of minor importance—a rise over last year's survey.

With a growing amount of data breaches and stepped up cybersecurity concerns related to COVID-19, along with increasing data privacy regulations, middle market companies must drive awareness throughout their organizations and take advantage of benchmarking opportunities to properly deploy generally limited resources. RSM has developed this report to provide insights into relevant middle market cybersecurity and data privacy trends, as well as strategies organizations can implement to strengthen security and privacy programs. ■

NETDILIGENCE RESEARCH EMPHASIZES THE MIDDLE MARKET CYBERTHREAT

The recent NetDiligence [1] Cyber Claims Study, sponsored by RSM, illustrates the level of focus that hackers are now placing on middle market companies. The report found that 96% of cyber insurance claims came from small to medium enterprises, with only 4% of claims coming from companies with over $2 billion in revenue. With this data, it is clear that criminals have zeroed in on the middle market.

Cyber insurance claims (2018)



Source: NetDiligence

Companies must prepare for the complete range of cybersecurity threats, as the most prevalent attack methods change over time. For example, the NetDiligence study showed that social engineering accounted for the highest amount of losses among middle market companies, overtaking ransomware, which was the leader in last year's report. Ransomware ranks second this year, followed by phishing and wire transfer fraud.

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

CYBERTHREATS CONTINUE TO EVOLVE, AND COMPANIES MUST BE PREPARED

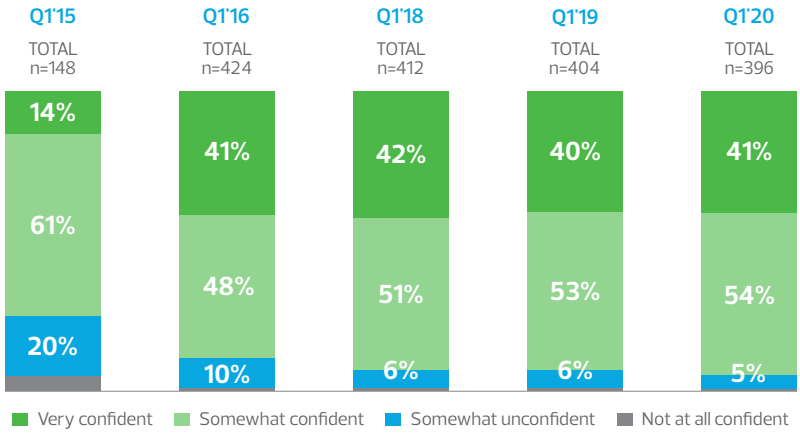
COVID-19 demonstrates how quickly risks can change

MORE COMPANIES than ever are confident in their organizations' current security measures to safeguard sensitive customer data, despite the consistent rise in data breaches and other cyber incidents. Cyberattacks evolve in an attempt to expose weaknesses, and that has never been more evident than this year during the COVID-19 pandemic. Middle market companies must be careful not to allow overconfidence in existing controls to create vulnerabilities to evolving threats.

The RSM MMBI survey found that 95% of middle market executives claim that they are confident in their current security stance, up 2% from last year's survey. However, the highest percentage of respondents in the history of the survey reported a data breach—18% compared to 15% last year and 5% six years ago. Threats can pivot quickly, and middle market protective controls sometimes fail to keep up.

Early 2020 is a prime example of how quickly threats can change and take advantage of vulnerabilities. As COVID-19 spread across the world and became a global pandemic, cybercriminals deployed persistent campaigns that capitalized on the uncertainty and fear related to the coronavirus and, in some cases, reduced cybersecurity measures because of the surge in employees working from home.

Confidence in current measures to safeguard data



Source: RSM US Middle Market Business Index survey, Q1 2020

"Attackers will always try to utilize scenarios that will make it most likely that targets will interact with their malicious emails, and leveraging disasters has unfortunately been one of their preferred methods." *– Daimon Geopfert, Principal, RSM US LLP*

"Unfortunately, during this historical pandemic, cyber thieves are preying on organizations," commented Ken Stasiak, RSM principal. "As companies address the new normal, we may see a spike in security breaches over the next several months."

Lawmakers have warned that the coronavirus pandemic has made the United States more vulnerable than ever to a serious cyberattack,[2] due to the increased attention paid to the crisis. These vulnerabilities extend to the middle market, where protections are simply not able to reach the level of government organizations or large international businesses. Threat actors are seeking attractive targets, and the reality is that nearly every company is at risk.

In the response to the COVID-19 pandemic, resources have shifted across the middle market, potentially taking attention away from security to focus on sustainability. In addition, employees using home networks can break the chain of security controls that have been developed within internal networks.

Phishing attempts represent the most prevalent method of attack during the COVID-19 pandemic. Emails are designed to look like they have guidance or advice from a company resource, or a legitimate organization, such as the World Health Organization or the Centers for Disease Control and Prevention. These messages attempt to coax recipients to click on a link or an attachment that launches malware to steal IDs and passwords that could lead to stolen company data.

Criminals have become very sophisticated, developing fake charities, and registering websites that seem closely aligned with COVID-19 news, relief or treatment. Their business is deception, and unfortunately, people will succumb to the tactics, especially in a time of crisis.

"Attackers will always try to utilize scenarios that will make it most likely that targets will interact with their malicious emails, and leveraging disasters has unfortunately been one of their preferred methods," said Daimon Geopfert, RSM principal and leader, national security, privacy and risk. "When people are stressed and afraid, they are not likely to use critical thinking, and this leads to a significantly increased failure rate of basic social engineering training where someone would ask 'do I know the sender?' or 'was I expecting this message.'"

These phishing scams are also leading to ransomware attacks, as attackers gain control of a company's network or steal company or customer records, and demand payment for their return.

Middle market companies are largely confident in their existing controls, likely because of increases in cyber insurance policies, training and dedicated resources to manage cybersecurity. But disaster responses are a unique scenario and often result in a new world of threats and demands on potentially strained resources. Even with a sharper focus on cybersecurity protections, it's difficult to stay ahead of threat actors.

The COVID-19 pandemic has caused several cybersecurity challenges, but it emphasizes how quickly criminals can strike and adjust strategies to take advantage of potential vulnerabilities. Middle market companies must be ready for any scenario by proactively communicating the risks, emphasizing where predators may be lurking, and adjusting security policies as necessary—such as in an extended remote working scenario.

"One of the biggest cybersecurity challenges companies face is the cultural shift or divide from a remote workforce," said Stasiak. "The effects of a divided workforce, now only connected via technology, allows potential attacks to exploit the trust of employees and flaws in technology to gain access to company resources." ■

2 "The Cybersecurity 202: Coronavirus pandemic makes U.S. more vulnerable to serious cyberattack, lawmakers warn," *The Washington Post*, accessed March 24, 2020.

INFORMATION AND DATA SECURITY

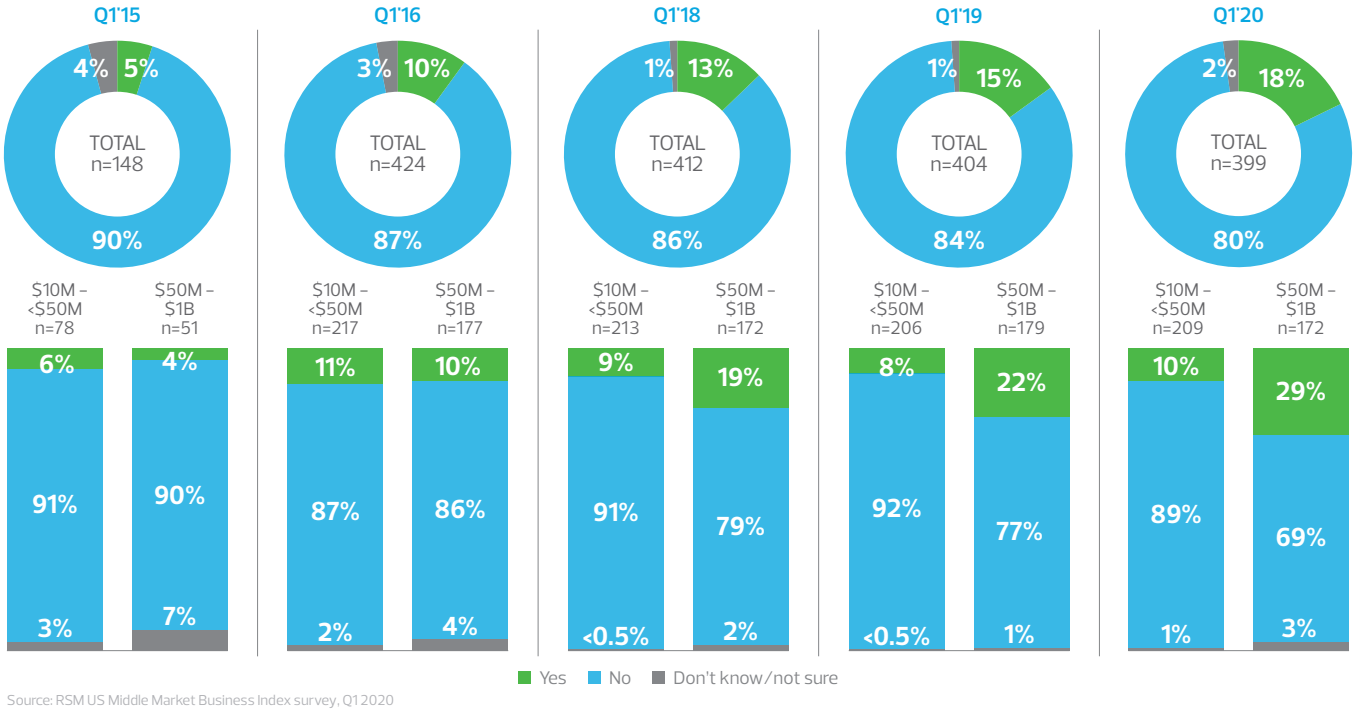
THE VALUE OF DATA has increased significantly in recent years, as companies have learned to use it as the foundation for strategic decision-making and overall corporate strategy. Unfortunately, that same data and intellectual property hold a high value to cybercriminals, as they can be sold on underground markets, held for ransom or even used in identity theft campaigns.

Unfortunately, all middle market companies will likely suffer a data breach—or already have. The combination of high-value data that middle market organizations possess, a lower level of security than large-cap organizations and evolving attack vectors has led to a rise in breaches in this segment of the market. Companies now understand the risks at hand, but staying ahead of the threat is challenging.

RSM's 2020 first quarter Middle Market Business Index survey polled 400 senior executives at middle market companies about their cybersecurity and data privacy challenges, providing a glimpse into the threats to the largest segment of the U.S. economy. In many cases, survey research provides specific data for smaller ($10 million to less than $50 million in revenue) and larger ($50 million–$1 billion in revenue) middle market organizations.

The survey shows that the threat to the middle market is growing, as the number of data breaches has risen, as it has each year since the MMBI survey began six years ago. This year, 18% of middle market executives disclosed that they experienced a data breach in the last year, up 3% from the 2019 report, and over three times the percentage since 2015.

Experienced data breach last year

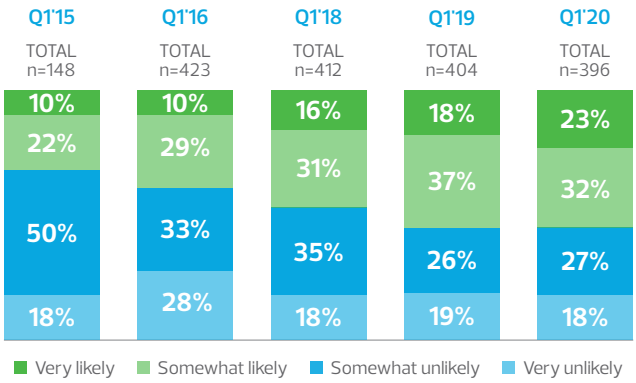


Source: RSM US Middle Market Business Index survey, Q1 2020

Organizations face a constant battle to outthink and out strategize criminals when developing data security strategies.

It appears that middle market executives know how widespread cybersecurity threats have become, as more than half of respondents (55%) indicated that an attempt to illegally access their data or systems is "very likely" or "somewhat likely" this year. This number is the same as in last year's survey, but a significant increase from just 32% six years ago.

Likelihood unauthorized users will attempt to access data or systems



Source: RSM US Middle Market Business Index survey, Q1 2020

Middle market companies are certainly attempting to address growing cybersecurity threats, as 71% of MMBI survey respondents reported having a dedicated function focused on data security and privacy, a 3% increase from last year. Not surprisingly, larger middle market companies are more likely to have a focused resource, with 76% reporting one compared to 69% of smaller counterparts.

"With the shortage for cybersecurity talent remaining high, it is important that companies continually address the shortage with outsourcing specific cybersecurity functions," Stasiak said.

Geopfert sees the environment for talented security personnel changing in the midst of the COVID-19 pandemic. "The current coronavirus situation is a double-edged sword," he said. "Some organizations that are hard-pressed for revenue inevitably release personnel, and unfortunately, security resources are often included into those cuts because they are not viewed as core to the business. In the long term, this does suddenly create a pool of security resources that are available for hire to organizations that had previously been struggling to find qualified personnel."

In addition, companies updated several security protocols in response to publicized data breaches at varying degrees. Seventy-one percent of respondents reported they updated security protocols, a 2% decline from last year. Furthermore, 55% purchased new or upgraded software, a 6% drop from the 2019 report. In fact, half of larger organizations detailed purchasing new or upgrading software, 12% less than last year.

Actions organization has taken due to publicized data security breaches

	Q1'19 TOTAL n=395	Q1'20 TOTAL n=385
Updated security protocols	73	71
Purchased new or upgraded software	61	55
Updated our privacy policies	55	53
Purchased new or upgraded hardware	47	48
Engaged data security consultants	42	43
Added data security staff	25	27
All of the above	11	6
Other	20	15
Took no action	NA	NA

Source: RSM US Middle Market Business Index survey, Q1 2020

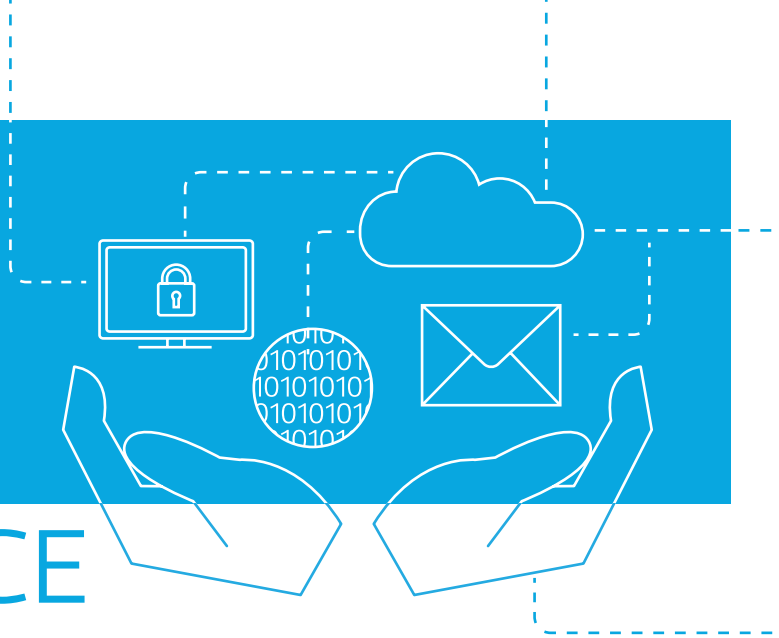
"With overall confidence being high in the ability for the security program to protect against cyberthreats, it is not surprising to see a drop-off in spending on security hardware and software," said Stasiak.

In the past, middle market companies typically underestimated the level and scope of potential cybersecurity threats, assuming that they were too small for their data to be of value. However, with the steady increase in cyber incidents and greater concern about breach attempts, companies now recognize the risks posed by cybercriminals. Organizations face a constant battle to outthink and out strategize criminals when developing data security strategies, but successful efforts can help avoid—or at least reduce—the costs associated with a potential breach. ■

MIDDLE MARKET INSIGHT

"Navigating cybersecurity risk begins with awareness and preparedness, which is what we are focusing on from the outset with our clients."

—Financial technology executive, RSM US MMBI Q1 survey



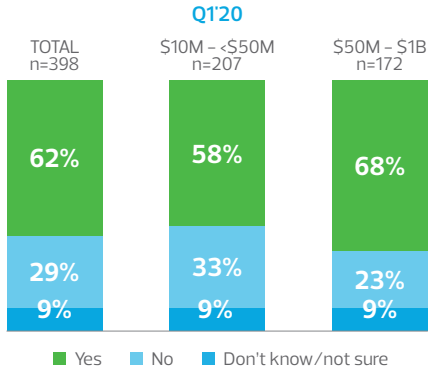
CYBER INSURANCE

AS THE FREQUENCY and scope of cyberattacks increase, cyber insurance has become a valuable protective measure for middle market companies. An effective policy can go a long way toward securing a company's data and offsetting any potential losses following a breach.

Cyber insurance is now an essential solution, combining with a comprehensive security program to safeguard sensitive data, intellectual property, finances and a company's reputation. However, a policy is only as strong as its coverages and limits, and companies must fully understand both of those elements.

The RSM MMBI survey found that 62% of middle market businesses currently claim to have a cyber insurance policy to protect their companies against internet-based risks, a 5% increase from last year's study. More of the larger middle market respondents (68%) invest in policies than smaller organizations (58%), but similar increases were seen in both segments from last year.

Organization carries a cyber insurance policy

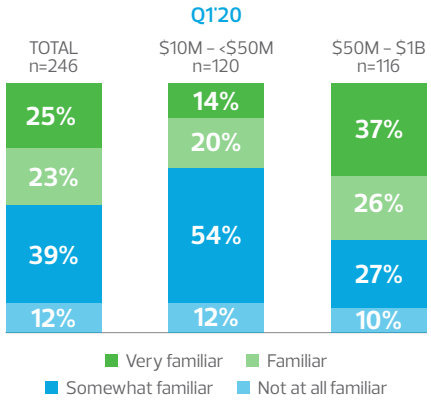


Source: RSM US Middle Market Business Index survey, Q1 2020

Optimally, cyber insurance policies are meant to fill in the gaps in traditional liability insurance, which typically excludes cyber coverage. It is imperative to understand how these two policies interact, and whether cyber policies address vulnerabilities. Otherwise, harmful areas of weakness can exist and losses may occur in areas that the company assumes they have coverage.

For example, even though the use of cyber insurance is increasing, less than half of companies are familiar with their coverages. Among middle market organizations that carry cyber insurance policies, 48% of executives report familiarity with their coverages, a 5% increase from last year. Smaller middle market companies appear most at risk, as only 34% of respondents in that category are familiar with their coverages, compared to 63% from larger organizations.

Familiarity with what organization's cyber insurance policy covers



Source: RSM US Middle Market Business Index survey, Q1 2020

This scenario can present significant challenges for middle market organizations, as providers have started making changes to coverages and excluding features that were covered in the past. Many providers were new entrants into the cyber insurance market, and it took a few years to understand how to properly price policies. After seeing how claims have been disbursed, some larger risk items are

Optimally, cyber insurance policies are meant to fill in the gaps in traditional liability insurance, which typically excludes cyber coverage. It is imperative to understand how these two policies interact.

no longer included in many policies. Therefore, companies must pay close attention to their policies to ensure they are properly covered.

"Cyber liability insurance is a safety net; however, you may want to make sure it doesn't have any holes in it before you fall," commented Stasiak.

Geopfert has seen firsthand how some companies struggle with cyber insurance. "We continue to run into organizations that make risky decisions with their security, often deferring investments and upgrades because they feel that cyber insurance will backstop their risk," he noted. "This has created some disastrous situations where their decisions led to incidents, or at least incidents that were more severe than they could have been, only to find out their policy did not include that type of event or all of the expected costs, or simply did not apply because their lack of controls violated the covenants of the policy."

With a similar design to general liability insurance policies, cyber insurance policy options are very broad in order to meet a wide range of specific needs. In RSM's survey, middle market executives report that their cyber insurance policies most often cover data destruction (74%), business interruptions (67%), hacking (65%) and extortion (65%). Interestingly, coverages for data destruction (83%), business interruption (77%) and hacking (78%) each declined from the results of the 2019 survey.

Other coverages also have experienced considerable reductions in the last year. For example, while theft and denial of service attacks were mentioned by 56% and 45% of respondents, respectively, the levels reporting coverage for these risks in cyber insurance policies are down significantly versus a year ago (71% and 61% in 2019).

Risks or exposures the cyber insurance policy covers

	Q1'19 TOTAL n=100	Q1'20 TOTAL n=120
Data destruction	83	74
Business interruption	77	67
Hacking	78	65
Extortion (including ransomware attacks)	62	65
Theft	71	56
Post-incident investigative expenses	57	52
Failure to safeguard data	59	51
Denial of service attacks	61	45
Post-incident public relations expenses	47	44
Defamation	38	31
None of the above	0	<0.5

Source: RSM US Middle Market Business Index survey, Q1 2020

"It's not too surprising to see a decrease in denial of service insurance coverage," commented Stasiak. "Given distributive technology such as the cloud, companies are feeling more confident in being isolated from denial of service attacks."

However, with so many middle market companies leveraging the cloud, Stasiak advises that those coverage levels require special attention. "Given the reliance of cloud providers, if a breach occurs are you protected even if your cloud provider was at fault?"

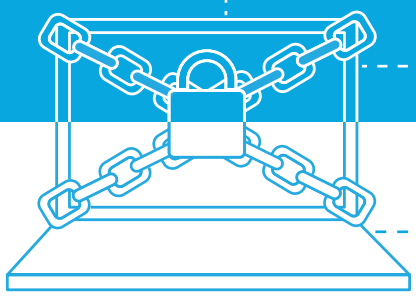
Cyber insurance is becoming a must-have solution for middle market companies, given the increases in data breaches and the subsequent costs—financial, reputational and regulatory—that victims can incur. However, companies must be careful when establishing or renewing policies to ensure that expected coverages are included. Experiencing a breach and then learning that an existing cyber insurance policy does not cover the losses can make a bad situation even worse. ■

MIDDLE MARKET INSIGHT

"Our top business problem is security. You can never truly be absolutely secured in this day and age."

—Technology executive, RSM US MMBI Q1 survey

RANSOMWARE ATTACKS



RANSOMWARE THREATS remain prevalent within the middle market, taking multiple forms and requiring businesses to take a more proactive stance to protect key data and intellectual property. Media reports of ransomware attacks in virtually every industry emerge on almost a daily basis, as deploying ransomware is relatively easy for criminals to execute with the potential for significant rewards.

Cybercriminals typically employ two different tactics for ransomware attacks. The first is a very basic strategy, repetitively sending fraudulent emails from fake or compromised accounts with no discernable pattern. The second is a more sophisticated campaign, specifically targeting vulnerable networks or systems.

Unfortunately, with more people generally working remotely or from home—especially in response to the COVID-19 pandemic—criminals have more access to vulnerable networks. In many cases, the majority of company workforces are working remotely, and remote desktops often do not have the same level of security protections as on-premise networks. In the rush to implement new remote policies, security may have been an afterthought, inadvertently creating low-hanging fruit for hackers.

Stasiak emphasized how the coronavirus crisis can further expose existing issues. "RSM conducted over 60 ransomware assessments following the issuance of last year's MMBI Cybersecurity Special Report," he said. "The top three controls that most organizations were lacking in defending a ransomware attack were:

1. Segmentation (83%)
2. Restricting and disabling end user's local admin privileges (75%)
3. Two-factor authentication for email (50%)"

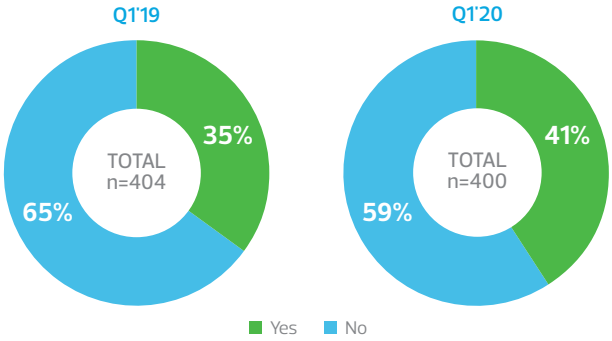
Once hackers gain access, they attempt to lock areas of the network or files that contain critical data. A message is sent detailing areas that have been encrypted, including a ransom note with the amount necessary to unlock files before they are destroyed. In many cases, businesses chose not to pay the ransom, but the effort required to regain access to files can be time-consuming and costly.

Ransomware has always represented a concern for middle market businesses, but the threat has escalated in recent years because stolen data has flooded the underground market, and may not have as much value as it had in the past. In a ransomware attack, the criminal is not necessarily concerned with selling stolen data, just collecting a payment for unlocking a network or data. This approach cuts out the middleman and is often much more lucrative.

As ransomware attacks expand, more middle market companies either know a peer that has experienced an attack, or have been a target themselves. The RSM MMBI survey showed that 41% of middle market executives know someone that has been the target of a ransomware attack, a 6% increase over last year's data.

Not surprisingly, the number of middle market companies that have suffered a ransomware attack has also increased. The MMBI study found that 23% of middle market executives claimed a ransomware attack or demand during the last 12 months, a 3% rise from the 2019 report. Significantly more executives at larger organizations reported an attack than smaller organizations (32% versus 14%).

Know anyone who has been the target of a ransomware attack



Source: RSM US Middle Market Business Index survey, Q1 2020

"Ransomware is the great equalizer. It can cause as much damage in a midmarket manufacturer as it can in a large financial institution." *– Daimon Geopfert, Principal, RSM US LLP*

In addition, 9% of respondents in the RSM survey reported multiple attacks. This is a fairly common strategy from criminals; once they breach a business and find that it's vulnerable, they smell blood in the water and will often attempt another attack.

"Ransomware is the great equalizer," said Geopfert. "It can cause as much damage in a midmarket manufacturer as it can in a large financial institution."

Stasiak provided insight into a key strategy to potentially offset the rise in ransomware attacks. "Conducting incident response tabletop exercises is an efficient and effective way for organizations to determine their ability to identify and respond to a ransomware attack," he said.

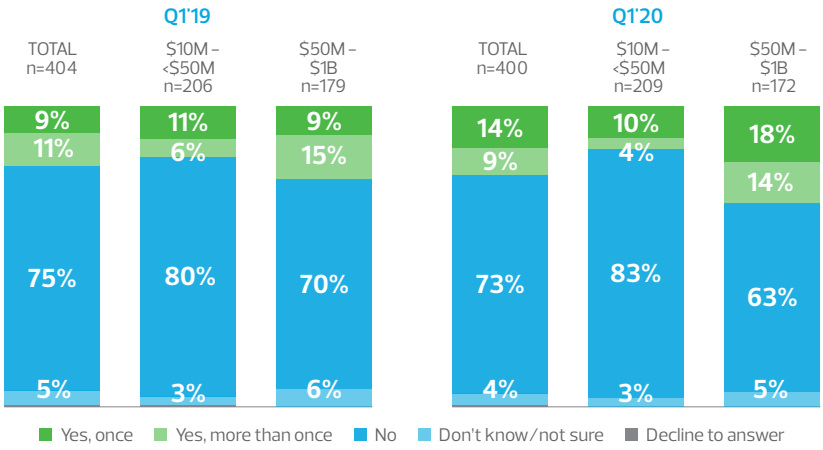
Many middle market executives are steadily recognizing the threat that ransomware poses. Forty-nine percent of middle market executives in the RSM survey see their organizations as likely targets for a ransomware attack, a 3% increase from last year's report and an 8% rise from two years ago. Executives at larger organizations are more likely than executives at smaller organizations to see the threat as very likely or somewhat likely (56% versus 43%).

MIDDLE MARKET INSIGHT

"Someone tried to breach our system, but we caught it early when a red flag was raised, and we were able to stop it before they could succeed."

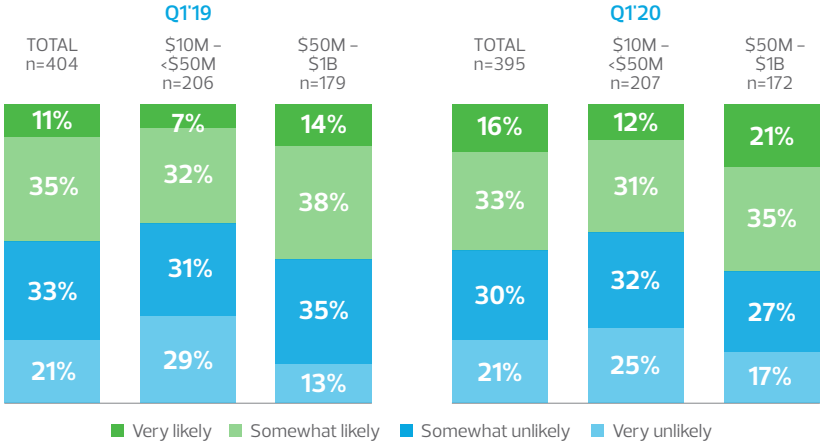
–Retail executive, RSM US MMBI Q1 survey

Experienced a ransomware attack or demand during the last 12 months



Source: RSM US Middle Market Business Index survey, Q1 2020

Likelihood organization at risk from a ransomware attack in the next 12 months



Source: RSM US Middle Market Business Index survey, Q1 2020

With its relative ease and potential high rewards, the ransomware threat shows no signs of relenting. In addition, with hackers not necessarily targeting a specific size or type of company, any organization is at risk. In order to combat ransomware, middle market organizations must implement a proactive security framework that includes increased awareness training throughout the organization that details common attack methods, incident response planning, system backups and patch management programs. ■

BUSINESS TAKEOVER THREATS

WHILE SOME CYBERATTACKS are complex and high-tech operations run by skilled hackers, many business takeover threats are low-tech efforts. Even so, they can cause just as much harm as more sophisticated incidents, and can be carried out by almost anyone. Social engineering and employee manipulation attacks fall into this category—simple, yet potentially very harmful incidents that are nearly impossible to avoid.

With the low level of expertise necessary to deploy, social engineering has become the most popular type of attack. In many of these incidents, an attacker contacts an employee directly—by email, phone or even in person—and attempts to manipulate that person into providing access to company credentials or sensitive data. The attacker may pose as a fellow employee, and seek to exploit a lack of security awareness to gain unauthorized access.

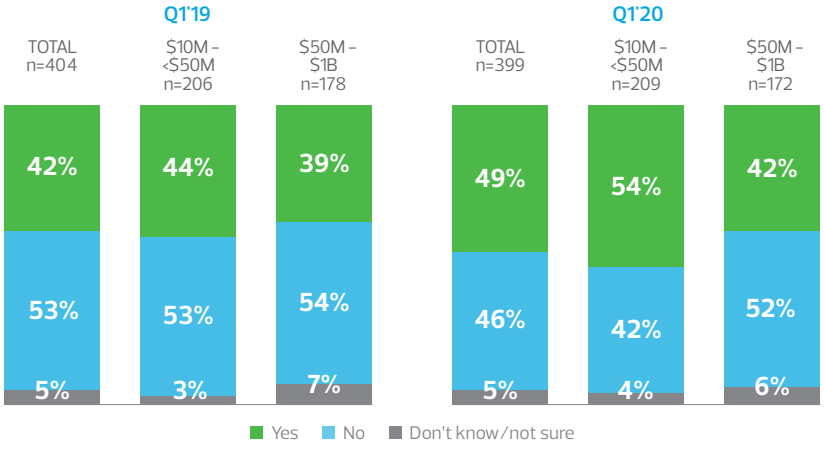
Phishing remains the most common social engineering strategy, with attackers sending emails that appear legitimate in an attempt to convince recipients to click on a corrupted link or attachment. In many cases, criminals gather data from company websites or social media profiles to make emails appear to have come directly from a trusted person.

However, the COVID-19 pandemic demonstrates how quickly phishing strategies can change. As the coronavirus spread, phishing attacks spiked with communications that appeared to be from esteemed organizations, including the World Health Organization and Centers for Disease Control and Prevention when, in reality, emails included malware or links to websites designed to collect information. Other schemes included fake emails to claim stimulus checks, or receive cures or vaccines.

With the relative ease of executing an attack, social engineering has become a persistent threat in the middle market. RSM MMBI research found that 49% of executives said that outside parties attempted to manipulate their employees into providing access to, or altering, systems, data or business processes by pretending to be trusted third parties or high-ranking company executives. This represents a 7% increase from last year's data.

In addition, executives from larger companies reported fewer of these attacks than those from smaller organizations, 42% versus 54% respectively.

Outside parties attempted to manipulate employees by pretending to be trusted third parties or company executives



Source: RSM US Middle Market Business Index survey, Q1 2020

"As organizations quickly conform to stay-at-home orders, ad hoc technology is being used to conduct essential business functions," commented Stasiak. "This untested and quickly implemented technology can pose significant risks to organizations."

A majority of middle market executives see the social engineering threat growing in the coming year. The RSM study found that 63% of respondents say their businesses are likely at risk of an attempt to manipulate employees in the next 12 months, roughly the same amount as last year.

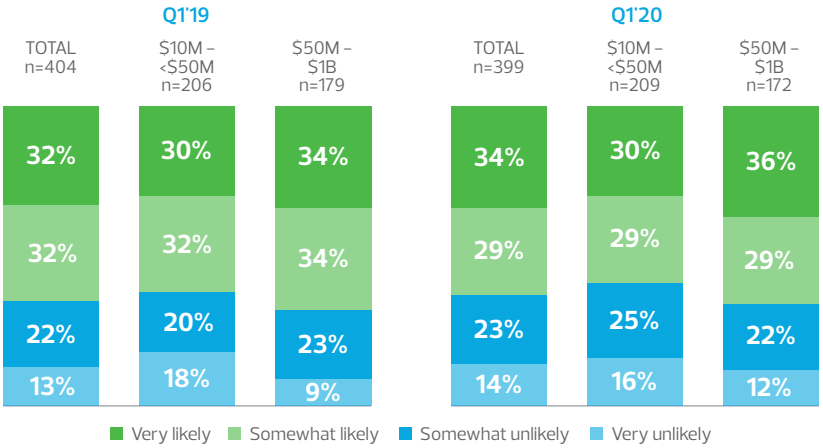
Social engineering attempts constantly occur, but luckily most are unsuccessful. However, the amount of successful attacks has increased significantly in the middle market, with 28% of executives in the RSM survey indicating attempts by outside parties to manipulate employees were successful, a sharp increase from 17% in the 2019 survey.

"Attackers are using the fear and confusion related to COVID-19 to create messages that are very likely to bypass casual inspection," said Geopfert. "For example, emails pretending to be from corporate HR announcing layoffs or changes to health benefits will often panic users into clicking on links or attachments without much caution. Also, the shift to a remote workforce has users operating out of their own homes, and just that simple change to a more casual environment can change user behavior toward being less attentive."

Stasiak offered a suggestion for companies attempting to protect themselves in a new work environment. "Now is the time to perform testing (phishing, penetration testing, etc.)," he said. "Don't wait for things to normalize, because the hackers won't."

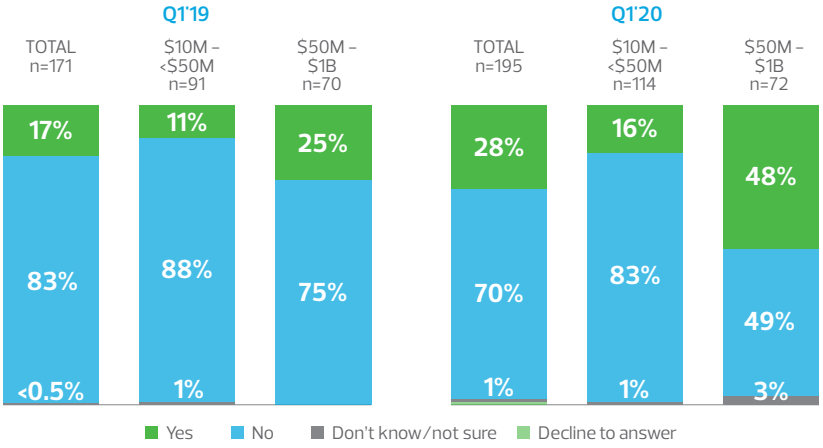
These attacks can take many forms, and therefore, companies must leverage several strategies to discourage them. Of the organizations in RSM's survey that experienced unsuccessful attacks, 90% listed employees not acting on the fraudulent request as a reason for the failed breach, a 7% drop from last year's survey. In addition, 66% of middle market executives said that secondary controls prevented the completion of an attack, and 46% acknowledged system controls that prevented delivery of fraudulent communications or materials to employees.

Likelihood organization at risk from attack by manipulating employees into providing access to business in the next 12 months



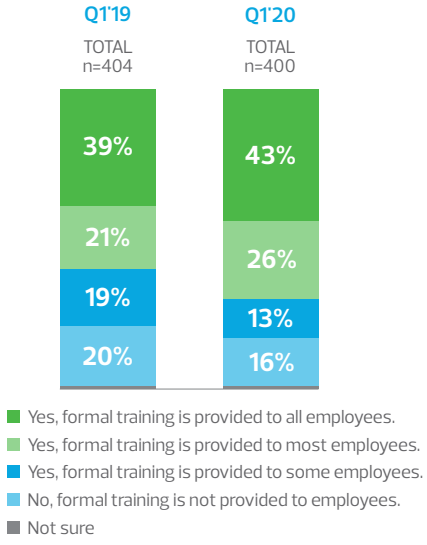
Source: RSM US Middle Market Business Index survey, Q1 2020

Attempts to manipulate employee(s) successful



Source: RSM US Middle Market Business Index survey, Q1 2020

Organization provides training on how to detect, identify and prevent attempts of unauthorized access



Source: RSM US Middle Market Business Index survey, Q1 2020

Training is typically the most effective defense against social engineering attacks, and the majority of middle market executives see the value in training. In the RSM survey, 82% of respondents reported their organization provides training to at least some employees on how to detect, identify and prevent attempts to gain unauthorized access to systems, data or business processes. This figure represents a 3% increase from the 2019 survey, but the remaining 18% of companies not offering training are likely at an increased risk.

"As more organizations implement awareness programs, we see a shift in the market from generalized phishing campaigns to specifically crafted phishes in order to keep pace with emerging threats," commented Stasiak. "This correlates with the decrease in employees' ability not to act on suspicious emails—down from last year's report."

PRIVACY PROTECTIONS COMPLIANCE

IN ADDITION TO the extensive cybersecurity challenges for middle market companies, the emerging data privacy laws also require significant attention. Middle market companies have long collected a significant amount of personal data to guide decision-making, with a focus on how to secure that data. However, now new privacy laws shift the discussion to why companies have that data in the first place.

The trailblazing legislation serving as the model for several subsequent data privacy laws around the world is the European Union's General Data Privacy Regulation. The GDPR took effect in May 2018, and created new data privacy rules for all companies that transmit, process or hold EU resident data, regardless of whether the company has European operations. Many companies were initially slow to adopt GDPR-compliant privacy programs, but after some significant enforcement actions, organizations generally understood the severity of the law.

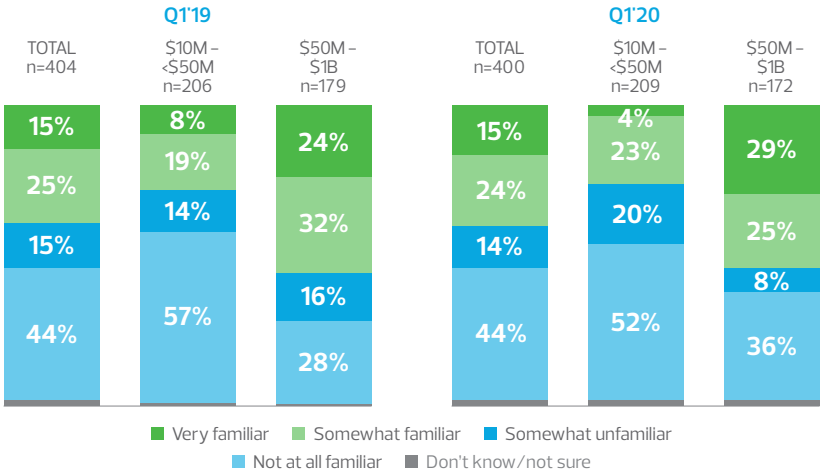
Nearly two years after implementation, the regulation is still generating large sanctions and fines for noncompliance. While the largest fine in the history of the GDPR was a $57 million penalty against Google in January 2019 for how it handled data, a $123 million fine against Marriott is currently under review due to a 2018 data breach.

The GDPR's success in protecting EU resident data has provided a blueprint for similar data privacy laws in several U.S. states. The Nevada Privacy Law went into effect Oct. 1, 2019, while the California Consumer Privacy Act became law Jan. 1 of this year. These regulations join existing laws in Massachusetts and Texas, and additional state laws will take effect this year. In addition, a federal privacy law is likely on the horizon, with multiple proposals introduced before Congress over the last year.

"Organizations need to be aware that privacy is the next wave of interruption to their business, and it is closer than many people assume," said Geopfert.

While many middle market companies are subject to GDPR regulations, only 39% of executives in the RSM MMBI survey say they are familiar with the requirements of the law, a slight drop from last year's data. Executives at larger organizations are more familiar with GDPR requirements than executives at smaller organizations—54% versus 27%.

Familiarity with requirements of the GDPR



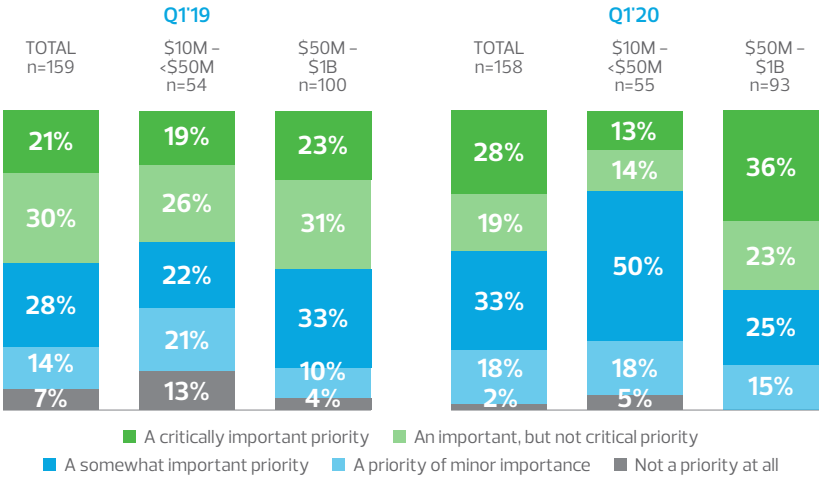
Source: RSM US Middle Market Business Index survey, Q1 2020

"With business processes changing overnight, the impacts to company's compliance programs and privacy have also changed. They need to continue to evaluate whether they are still compliant." *– Ken Stasiak, Principal, RSM US LLP*

With data privacy regulations already established in parts of the United States and additional guidelines in the planning phases, many middle market executives recognize that they will likely be subject to new laws soon. Among RSM survey respondents familiar with GDPR regulations, 83% believed their organizations will likely have to comply with privacy legislation similar to GDPR at a state or federal level in the United States during the next two years, a 5% increase from the 2019 survey.

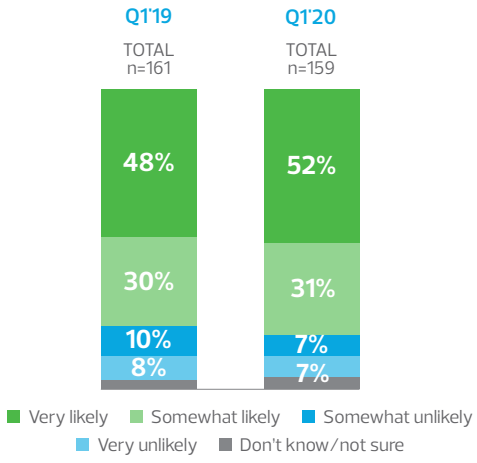
"With business processes changing overnight, the impacts to company's compliance programs and privacy have also changed," said Stasiak. "They need to continue to evaluate whether they are still compliant," said Stasiak.

How much of a priority is preparing for emerging privacy legislation or regulation



Source: RSM US Middle Market Business Index survey, Q1 2020

Likelihood organization will have to comply with privacy legislation during the next two years



Source: RSM US Middle Market Business Index survey, Q1 2020

Middle market executives are taking data privacy seriously and implementing plans to comply with future regulations. In fact, 98% of middle market executives who are familiar with GDPR regulations reported that preparing for emerging privacy legislation or regulation in the United States is a priority, a 5% increase from last year's report. Furthermore, 100% of larger organizations are prioritizing data privacy preparations.

Data privacy regulations have been a success overseas, and they represent a movement that is gaining steam in the United States at a rapid pace. With growing pressure on companies to protect customer data, there is no doubt that additional guidelines and regulations are coming soon. To reduce the likelihood of potential sanctions, middle market companies can prepare for potential upcoming legislation by becoming more familiar with the existing regulations that will likely serve as the basis for future laws.

MIDDLE MARKET INSIGHT

"Federal and state regulators continue to pepper financial institutions with new regulations, tools and guidance. Many institutions are struggling to keep up with even the basic tenets of a cybersecurity risk management policy or program."

–Financial technology executive, RSM US MMBI Q1 survey

MIGRATION TO THE CLOUD TO ENSURE DATA SECURITY

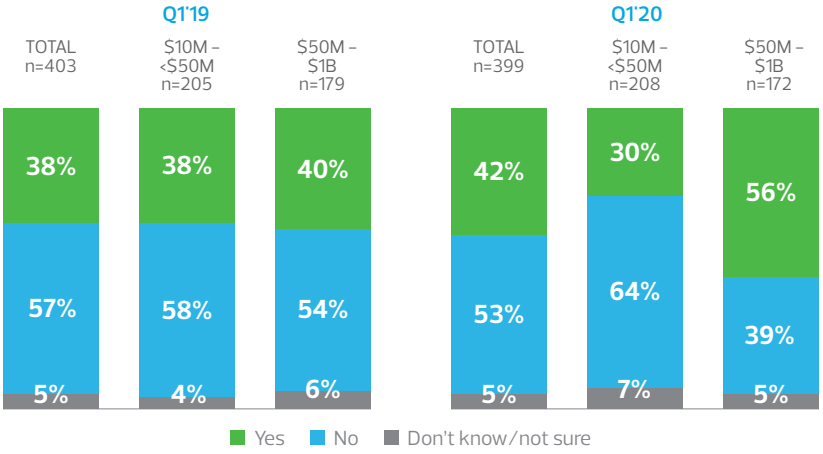
IN THE MIDDLE MARKET, the cloud offers an invaluable solution to gain more control over data, helping companies to understand how much data they have and where exactly it resides. However, in addition to better efficiency and access to data, middle market companies are also transitioning information and applications to the cloud to enhance security. The cloud offers several storage options, many with more extensive security capabilities than typical middle market companies have access to.

"Cloud solutions have a variety of packages and components," said Stasiak. "Like anything, companies must make sure that they understand what is turned on, and what is being used by selected cloud services."

Geopfert described the importance of implementing accurate security measures when moving to the cloud. "Cloud solutions can often simplify security configuration, monitoring and even compliance, but like any technology, companies need to understand how to deploy these solutions in a secure manner," he detailed. "Organizations tend to move onto these platforms without fully understanding what they are getting themselves into, and several large data breaches have been a result of simple misconfigurations within cloud solutions."

RSM MMBI data continues to show the gradual shift of middle market data to the cloud to strengthen security. The report shows that 42% of businesses moved or migrated data to the cloud as a result of security concerns, a 4% increase from last year's data. An increasing number of larger organizations are moving to the cloud because of security than smaller organizations—56% compared to 30%.

Organization moved or migrated data to the cloud for security concerns during the past year

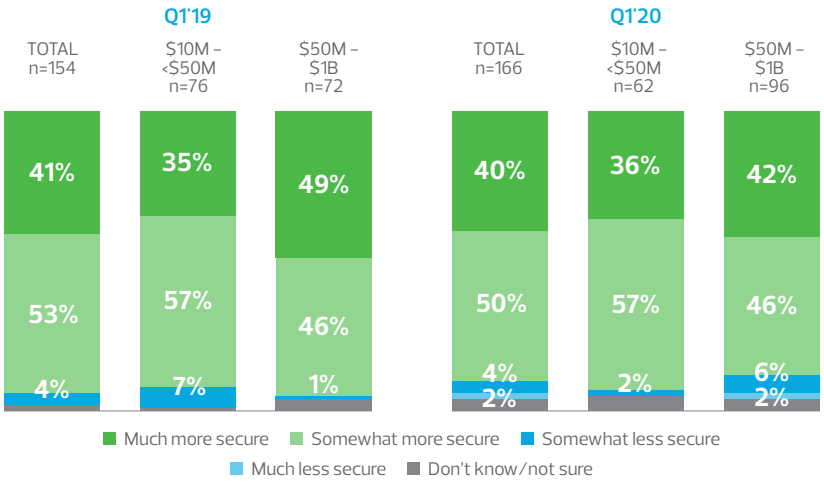


Source: RSM US Middle Market Business Index survey, Q1 2020

Middle market executives are largely comfortable with their data residing in the cloud, although confidence has slightly slipped compared to 2019 data. Among middle market executives reporting moving data to the cloud for security concerns, 90% believe the data residing in the cloud is more secure. This represents a 4% drop from last year's survey.

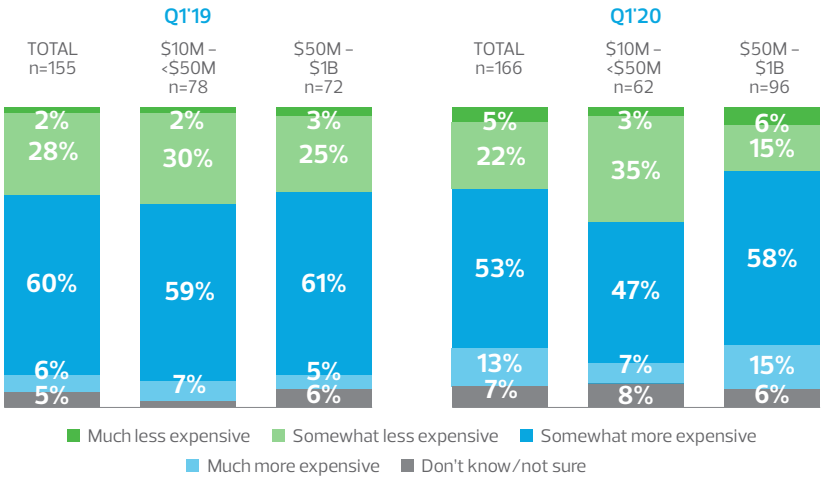
"Cloud solutions can often simplify security configuration, monitoring and even compliance, but like any technology, companies need to understand how to deploy these solutions in a secure manner." *– Daimon Geopfert, Principal, RSM US LLP*

Actual impact of moving data to the cloud due to security concerns



Source: RSM US Middle Market Business Index survey, Q1 2020

Cost impact of maintaining data in the cloud due to security concerns



Source: RSM US Middle Market Business Index survey, Q1 2020

Stasiak provided a quick tip for companies to potentially increase confidence in cloud solutions. "Organizations should include cloud providers in their incident response program. If the provider has an incident, do companies have the ability to engage and respond to potential effects to their data?"

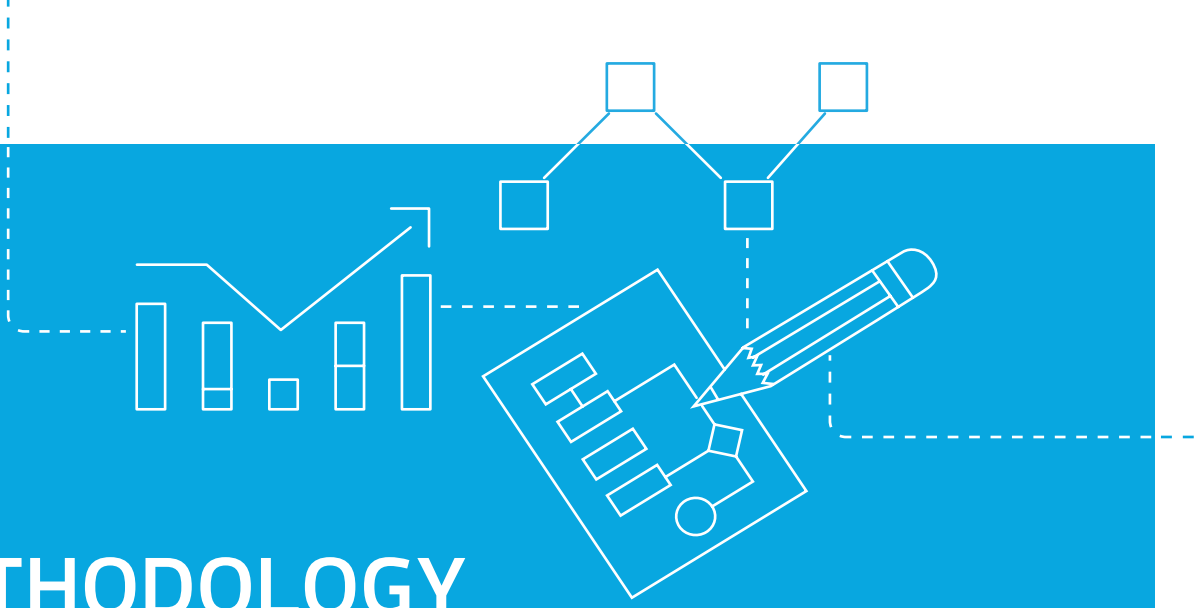
Another key reason middle market organizations move to the cloud is for cost savings, as hosting companies often offer more affordable storage options because of capacity and economies of scale. For example, the survey found that 27% of middle market executives who moved data to the cloud for security concerns indicated that the solution is less expensive, a 3% decrease from last year's data.

While the cloud can provide significant benefits, middle market companies must be careful when selecting a cloud provider. Organizations should go through a thorough due diligence process on potential providers to confirm that their security capabilities and access levels match demands. At the end of the day, the company that owns the data is still responsible if a breach occurs, and incidents in the cloud can be more difficult to remediate.

"Companies must ensure that cloud providers are enrolled in their third-party vendor management program, and are following their guidance on how to protect the data they are storing," commented Stasiak.

Beyond the cloud, a growing number of middle market companies are considering adding blockchain technology to enhance their security and privacy efforts. The RSM MMBI survey found that 29% of respondents are pursuing blockchain technology solutions to ensure security or privacy of data, a 7% increase from a year ago. More of the larger middle market organizations are evaluating blockchain than smaller peers—47% compared to 15%.

The cloud and blockchain provide innovative options for middle market organizations to store data more securely than on-premise solutions. However, organizations must be careful when selecting providers to ensure that potential platforms match security demands, and do not result in additional gaps or vulnerabilities. ■



METHODOLOGY

ABOUT THE RSM US MIDDLE MARKET BUSINESS INDEX RESEARCH

The RSM US Middle Market Business Index survey data in the first quarter of 2020 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; the 2020 first quarter survey was conducted from Jan. 13 to Jan. 31, 2020. Information was collected by phone and online survey from 400 executives, including 233 panel members and a sample of 167 online respondents. Data are weighted by industry.

U.S. CHAMBER OF COMMERCE

RSM

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

RSM

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