RSM US MIDDLE MARKET BUSINESS INDEX

# CYBERSECURITY

SPECIAL REPORT


U.S. CHAMBER OF COMMERCE

RSM

RSM US MIDDLE MARKET BUSINESS INDEX

# CYBERSECURITY

## SPECIAL REPORT 2019

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**

# THE MIDDLE MARKET REALIZES THE CYBER THREAT BUT UNCERTAINTY REMAINS

Cybercrime has become a reality for the middle market. While major cyber incidents and data breaches at large corporations such as Marriott and Facebook continue to capture global headlines, middle market companies are starting to recognize that they are often the prime target for cybercriminals.

In the past, midsize companies often held the perception that they were too small to be a target for hackers. However, with rising concern across the board about several types of cybersecurity attacks uncovered in the RSM US Middle Market Business Index survey, these companies are starting to take notice.

According to first quarter 2019 MMBI data, 15 percent of middle market C-suite executives said their companies experienced a data breach in the last year, up from 13 percent in 2018 and a significant jump from 5 percent just four years ago. Larger middle market organizations continue to be most at risk, with high volumes of valuable data to attract cybercriminals, but lacking the robust security resources of their large-cap peers.

However, the focus on data breaches can be misleading, as the term data breach typically entails a cyber incident resulting in stolen sensitive data. A wide variety of cyber incidents does not result in theft of data, such as ransomware, which interrupts business operations or types of social engineering that could cause the direct theft of funds from bank accounts.

There are few signs that the cybersecurity threat is relenting; in fact, even amid increased attention and investment toward security, it continues to grow. Over half of middle market executives surveyed indicated it is likely that unauthorized users will attempt to access their organization's data or systems in 2019.

In an effort to protect their firms and individual users against cybersecurity threats, more than half of midsize companies report carrying cyber insurance. However, among those organizations with coverage, only 43 percent of executives claim familiarity with policy details.

In addition to cybersecurity challenges, emerging data privacy regulations are requiring organizations to make a significant shift in how they collect and store data. The European Union's General Data Privacy Regulation, known as GDPR, took effect in May 2018. Similar legislation is emerging in the United States, led by the California Consumer Protection Act, and congressional hearings have discussed regulation at the federal level.

The new laws do not focus on how companies protect data, but rather why they have it in the first place, and these regulations create an array of new business challenges for organizations highly reliant on customer data. As data privacy moves to the forefront, only 40 percent of executives report familiarity with the guidelines of GDPR or other privacy regulations.

Cybersecurity threats to the middle market are very broad and evolving. The 2018 NetDiligence[1] Cyber Claims Study, sponsored by RSM, showed ransomware has become the most common form of cyber incident, but traditional hacking, malware and business email compromises are still very popular with attackers. Organizations must develop cybersecurity strategies that consider several threats to limit the risk of as many varieties of these attacks as possible.

**While major cyber incidents and data breaches at large corporations continue to capture global headlines, middle market companies are starting to recognize that they are often the prime target for cybercriminals.**

Other studies, such as the Identity Theft Resource Center's[2] 2018 End of Year Data Breach Report, also show that the number of data breaches actually fell last year by 23 percent. RSM's survey shows that criminals show no signs of backing down in the middle market, but they are slowly shifting from attacks meant to steal data to those meant to extract payment directly from the victim. Attacks come by several means: forcing the victim to pay a ransom, stealing funds by compromising corporate bank accounts or tricking the victim into making fraudulent payments.

With generally limited resources, middle market organizations must place a premium on awareness and benchmarking to help mitigate the threat of cybersecurity attacks and to comply with data privacy regulations. RSM has developed this report to provide insights into relevant middle market cybersecurity and data privacy trends, and to highlight steps companies can take to enhance security and privacy efforts.

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.

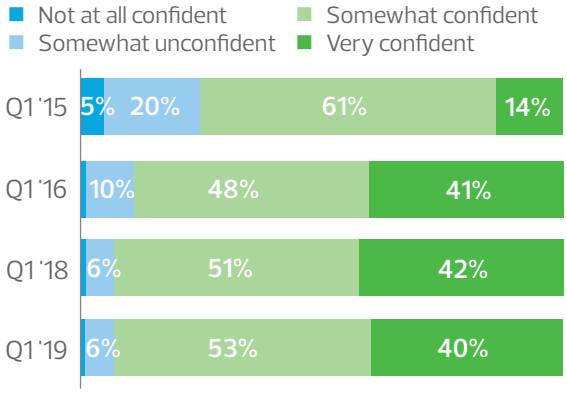
2 The Identity Theft Resource Center is a nonprofit organization established to support victims of identity theft and to broaden the awareness of identity theft, data breaches, cybersecurity, scams and fraud, and privacy issues.

# Growing confidence **CONFLICTS** with rising cyber concerns

Despite more middle market companies experiencing a data breach or other cyber incident in the last year, and rising levels of concern over future attacks, almost all of the executives polled in RSM's research are confident in their current security measures. While a high level of confidence may sound positive on the surface, overconfidence could mask potential vulnerabilities and a lack of communication to the C-suite.

RSM's survey found that 93 percent of middle market executives claim that they are confident in their organization's measures to safeguard sensitive customer data or their own environments for the second consecutive year. While the number of reported breaches has tripled over the last five years, the level of confidence expressed by executives has actually grown by 18 points. This creates a potentially dangerous situation where executives have a false sense of security, seeing their peers falling victim to attacks but fully believing that "it can't happen to us."

Confidence in current measures to safeguard data




Increased spending on information security is one potential reason for a high level of confidence. A research study from Gartner projected that worldwide spending on information security products and services would grow 12.4 percent in 2018 and an additional 8.7 percent in 2019.[3] We have found that middle market companies are indeed making larger cybersecurity investments, but many need to implement more defined plans to ensure the right products and services are chosen.

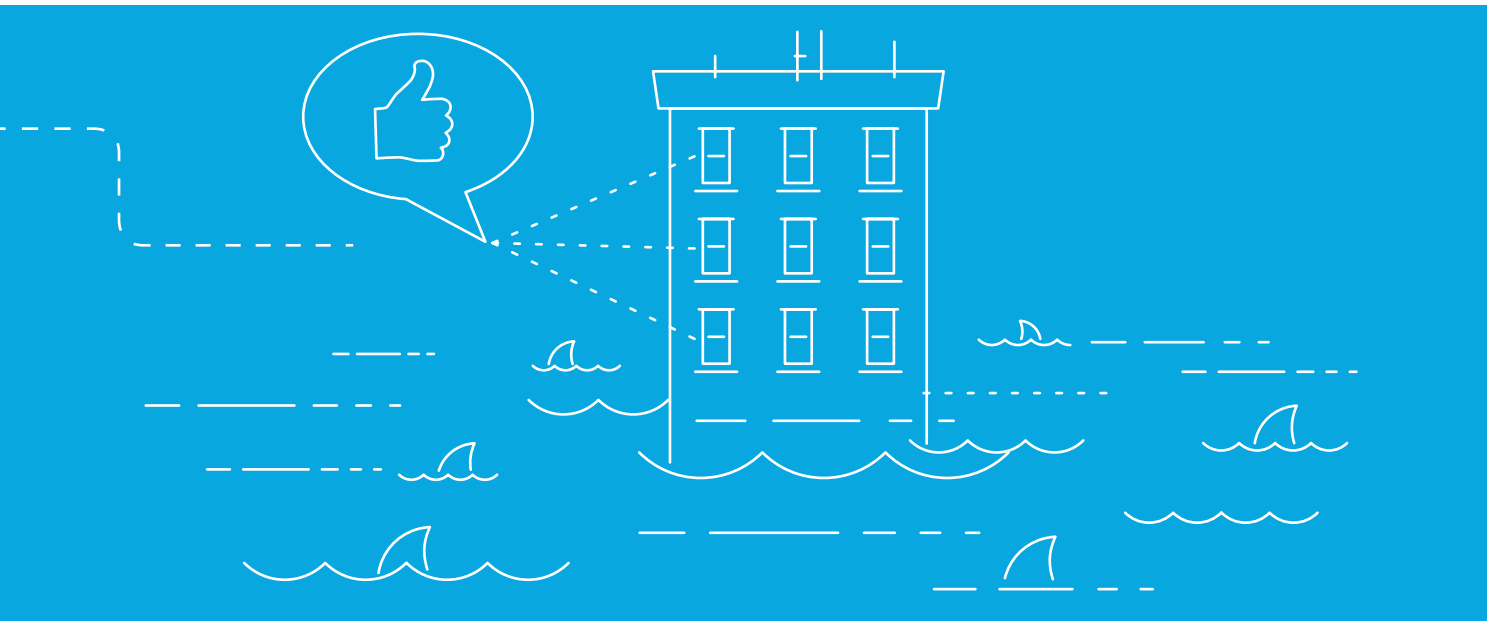
"More funds are being directed to information security, which seems like a positive on the surface," commented Daimon Geopfert, RSM principal and leader, national security, privacy and risk. "However, that strategy does not often translate into an actual improvement in an organization's security posture without significant effort put into deployment and configuration. Most security tools are only moderately useful out of the box, and getting full value from your purchase requires extensive changes in the environment and business processes."

In addition, many middle market companies have aligned their processes to an established information technology security framework, whether due to regulatory compliance obligations or in an effort to improve their security posture. Common frameworks include the National Institute of Standards and Technology Cybersecurity Framework, also known as the NIST CSF, as well as the International Organization for Standardization 27000 family of standards and the Payment Card Industry Data Security Standard. In fact, Gartner estimates that nearly 50 percent of U.S. organizations will adopt the NIST CSF by 2020.[4]

However, while mapping controls and functions to one of these frameworks is an effective first step, it does not mean that an organization is fully secure. These standards are meant to provide a strong foundation for information security, but companies must also consider several additional elements based on their specific industry and

3 "Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019," Gartner, accessed March 21, 2019, https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019.

4 "Cybersecurity Framework," National Institute of Standards and Technology, accessed March 21, 2019, https://www.nist.gov/industry-impacts/cybersecurity.



business objectives. Adopting a security framework can provide a sense of security, but not further adjusting it to the business can create security gaps.

"Aligning your security program to an accepted framework is a great first step, but these frameworks are a measure of completeness rather than effectiveness," commented Geopfert. "They generally turn into great checklists to validate that you have the major parts of a security program, but those parts then must be heavily tailored to your environment. Otherwise, you end up with the appearance of a security program that, in reality, isn't actually effective."

Finally, communication breakdowns can occur among executives, the board and the people on the ground who are implementing security processes and controls. Sometimes what is communicated to the board is a vastly different view than the perception of security inside the data center. Organizations must ensure their stakeholders are on the same page from top to bottom to properly understand and address potential security issues.

"In my opinion, information filtering in cybersecurity accounts for a large percentage of the confidence executives feel about their cybersecurity posture," commented Ken Stasiak, RSM principal and leader of security transformation services.

Stasiak finds that the executive level's view of the state of the security program often deviates significantly from the security and IT personnel's view of the program, often due to metrics and reporting processes that were not built to handle the nuances of modern security threats.

> "Aligning your security program to an accepted framework is a great first step, but these frameworks are a measure of completeness rather than effectiveness. They generally turn into great checklists to validate that you have the major parts of a security program."
>
> *– Daimon Geopfert, principal, RSM US LLP*

"For example, a security assessment may show dozens of low-risk issues and one very high-risk issue," said Stasiak. "Standard reporting approaches abstract these findings as they move from low-level IT teams, through management, and eventually to the executive layer. Eventually, that single high-risk finding is built into a summarized result, creating an overall low score. This approach might be appropriate for various areas of risk management, but often masks serious cybersecurity issues."

Our research shows that the threat to the middle market is growing, but the organizations now in cybercriminals' sights have only become more confident in current protections. Generally, companies have taken steps to improve cybersecurity, but criminals are becoming more sophisticated and determined. Middle market businesses must ensure that security investments, controls and communications align with rising threats, and that current actions do not create a false sense of security.

# INFORMATION AND **DATA SECURITY**

A company's data is often its most valuable asset, as volumes of internal and client information help to guide organizational decision-making and overall corporate strategy. However, that same data is coveted by hackers and other cybercriminals who seek to access and exploit sensitive customer and employee data, and intellectual property.

Middle market organizations have historically underestimated the value of their data and subsequently the threats to their information and systems. With the amount and severity of attack vectors growing and the value of information steadily on the rise, all organizations will likely experience a breach attempt or event—or already have.

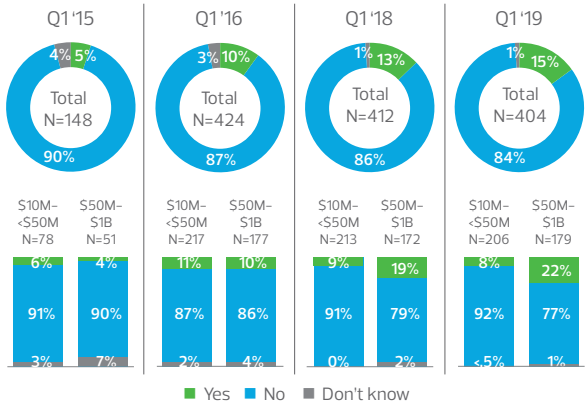
RSM's 2019 first quarter Middle Market Business Index survey polled 404 senior executives at midsize companies about their cybersecurity challenges, providing an overview of the threat to the largest segment of the U.S. economy. In many cases, survey research provides more specific data for smaller ($10 million to less than $50 million in revenue) and larger ($50 million–$1 billion in revenue) middle market organizations.

The survey shows that data breaches in the middle market continue to rise. Fifteen percent of middle market executives disclosed that they experienced a data breach in the last 12 months, triple the amount from just four years ago and up 2 percentage points from last year.

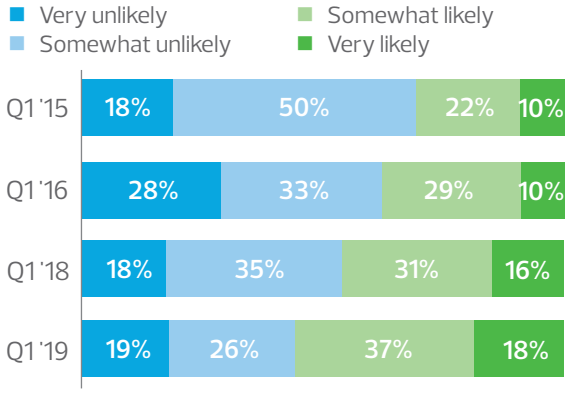
Once again, the middle market is a primary target—if not the focal point—for cybercriminals. The NetDiligence® 2018 Cyber Claims Study found that 61 percent of cyber insurance claims in 2017 were from companies with less than $50 million in revenue, with another 21 percent from companies with revenue of $50 million to $300 million. Altogether, companies with revenue under $2 billion accounted for 88 percent of claims in 2018.

Consistent with this continued threat, over half of middle market executives (55 percent) in RSM's research indicated an attempt to illegally access their companies' data or systems is either "very likely" or "somewhat likely" this year. This number is a significant increase over the 47 percent that answered in the same manner last year and from 32 percent five years ago.

## Companies experiencing data breaches in last 12 months



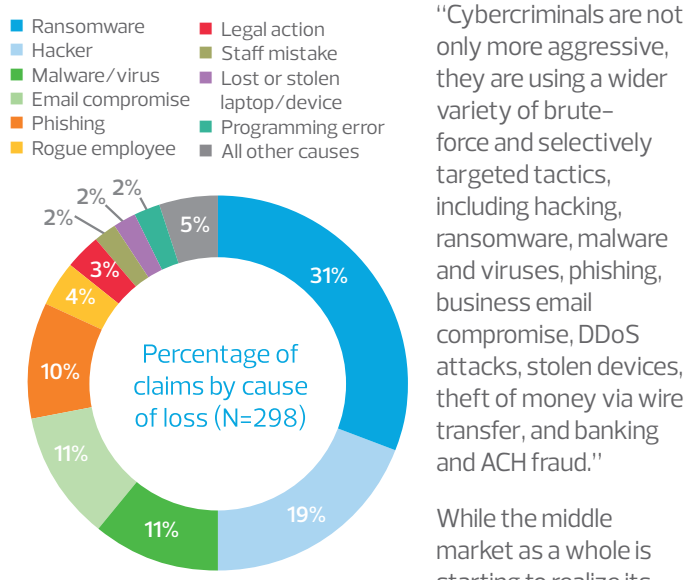

## Likelihood unauthorized users will attempt to access data/systems




As many middle market organizations have unfortunately found, the costs related to a data breach can be significant. For example, NetDiligence's research showed the average breach cost submitted for cybersecurity claims in 2017 was $604,000, with $60,900 as the median. However, financial costs cannot be the only consideration with a data breach, as the reputational costs and potential ongoing regulatory sanctions can be much more damaging.

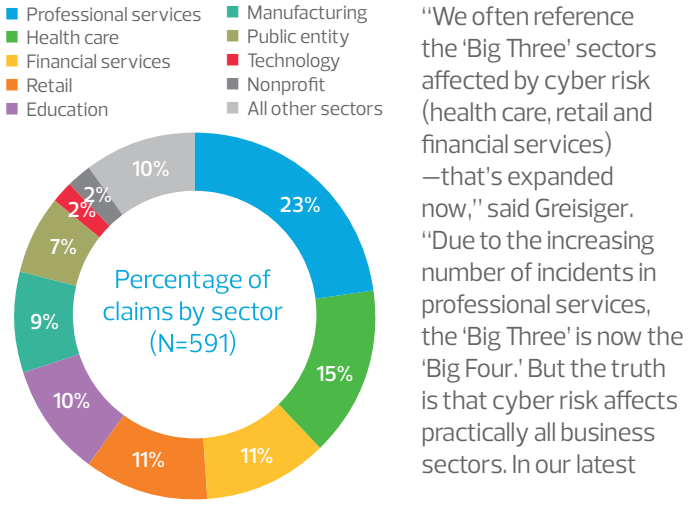
Ransomware has become the most popular breach method for cybercriminals, but several additional threats are prevalent in the middle market. In the NetDiligence survey, ransomware was responsible for 31 percent of losses, but hackers (19 percent), malware and viruses (11 percent), business email compromise (11 percent) and phishing (10 percent) also represented a significant amount of losses.

"In our latest study, 92 percent of cyber claims were attributable to criminal activity," said Mark Greisiger, NetDiligence president. "Cybercriminals are not only more aggressive, they are using a wider variety of brute-force and selectively targeted tactics, including hacking, ransomware, malware and viruses, phishing, business email compromise, DDoS attacks, stolen devices, theft of money via wire transfer, and banking and ACH fraud."




Source: 2018 NetDiligence Cyber Claims Report

While the middle market as a whole is starting to realize its vulnerability to cyber risks, individual industries must also understand that they are also at risk. NetDiligence research found that professional services (23 percent) and health care (15 percent) reported the largest amount of cyber claims. The financial services (11 percent), retail (11 percent), education (10 percent) and manufacturing (9 percent) industries also accounted for a significant number of claims.




Source: 2018 NetDiligence Cyber Claims Report

"We often reference the 'Big Three' sectors affected by cyber risk (health care, retail and financial services) —that's expanded now," said Greisiger. "Due to the increasing number of incidents in professional services, the 'Big Three' is now the 'Big Four.' But the truth is that cyber risk affects practically all business sectors. In our latest study, almost half the incidents (41 percent) occurred in sectors outside the Big Four."

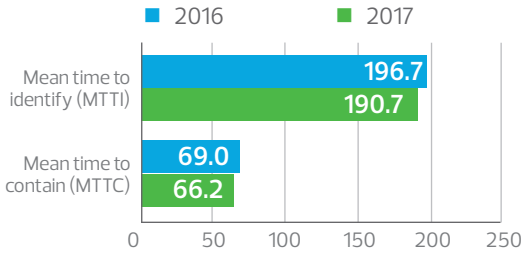
As technology evolves, threats will continue to grow and gain complexity. For example, 5G communications is on the horizon, bringing more connectivity for individuals and companies, but also more access points for cybercriminals. 5G will enable smart cities, and entire locales (such as Atlanta in 2018) have already been hacked, requiring millions in investments to strengthen cybersecurity policies. With the need to adopt emerging technology, the middle market must be prepared, with proactive security measures in place.

"Disruptive technology says it all," commented Stasiak. "Innovation can be very challenging for cybersecurity, so make sure to consider your controls when making decisions on new and emerging technology."

Geopfert also sees the increased threats emerging technology can present to middle market companies. "Organizations are still struggling with the increased connectivity into their environment made possible by high-speed internet, remote workers, cloud solutions and mobile devices," he said. "Technologies like 5G have the potential to completely dissolve what is left of the network boundary."

In a breach scenario, efficient identification and containment can limit data exposure, and financial and reputational losses. Unfortunately, the Ponemon Institute's 2018 Cost of a Data Breach Study reports the mean time to identify breaches in 2018 was 196.7 days, while the mean time to contain breaches was 69 days—both increased over 2017 as criminals continue to perfect their methods.

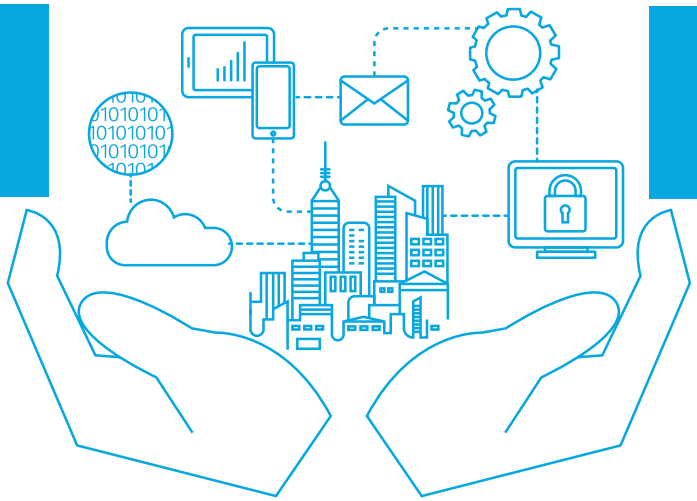
Days to identify and contain data breach over the past year




Source: 2018 Cost of a data breach study: Global overview, Ponemon Institute

With more middle market companies experiencing cyber incidents and exhibiting greater concern over potential risks, companies now have a better understanding of the cybersecurity threats they are facing. These companies—typically limited in resources—must still focus on developing or refining a cybersecurity framework that can protect internal and customer data, identify and address threats, and scale to encompass emerging technology, business expansion efforts and other related challenges.

# CYBER INSURANCE

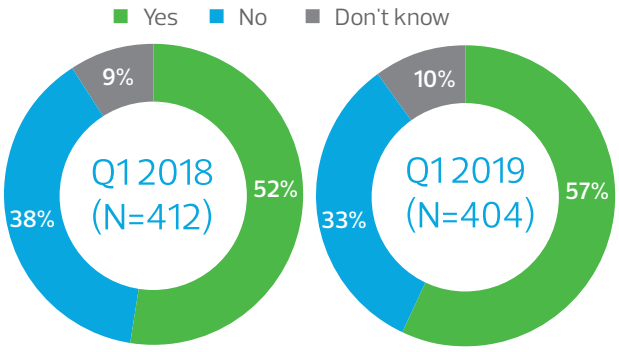


With the potential financial and operational impact of a data breach, cyber insurance is now a critical element of many middle market cybersecurity strategies. As leveraging data is now essential for corporate growth—carrying more value and therefore, more risk—companies are making additional investments to protect that information.

Cyber insurance is typically an effective solution for middle market organizations, working in concert with a comprehensive security program to implement a higher level of protection for sensitive data, finances and company reputation.

The RSM survey found that 57 percent of middle market businesses currently utilize a cyber insurance policy to protect their company against internet-based risks, up from 52 percent in last year's study. More of the larger middle market companies (63 percent) invest in policies than smaller organizations (53 percent), but usage rose in both segments from last year.

Organization carries a cyber insurance policy



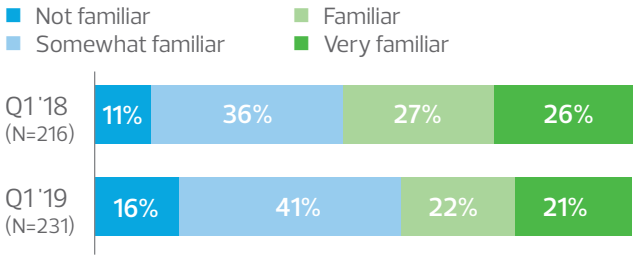

"Ensure your policy has specific requirements for penetration testing, security monitoring and others, and confirm you are meeting those obligations. If you violate the requirements of the policy, the insurer can claim that the policy is not in effect."

*— Daimon Geopfert, principal, RSM US LLP*

Cyber insurance policies are meant to fill the gaps left from traditional general liability insurance, which typically excludes cyber coverage. Organizations must understand how these two policies work together, otherwise potentially harmful vulnerabilities can exist and some losses may remain uncovered. Some companies assume they are covered by one of their policies, but then experience an event that falls in between the cracks in coverage.

For instance, while more middle market companies are utilizing cyber insurance, many do not understand how they are covered. RSM found that 58 percent of the companies that carry policies are familiar with their coverage levels, while 41 percent are somewhat familiar or not at all familiar. Smaller middle market companies appear most at risk, as only 30 percent of companies are familiar with their coverage, a 21 percentage point drop from just last year.

### Familiarity with what organization's cyber insurance policy covers

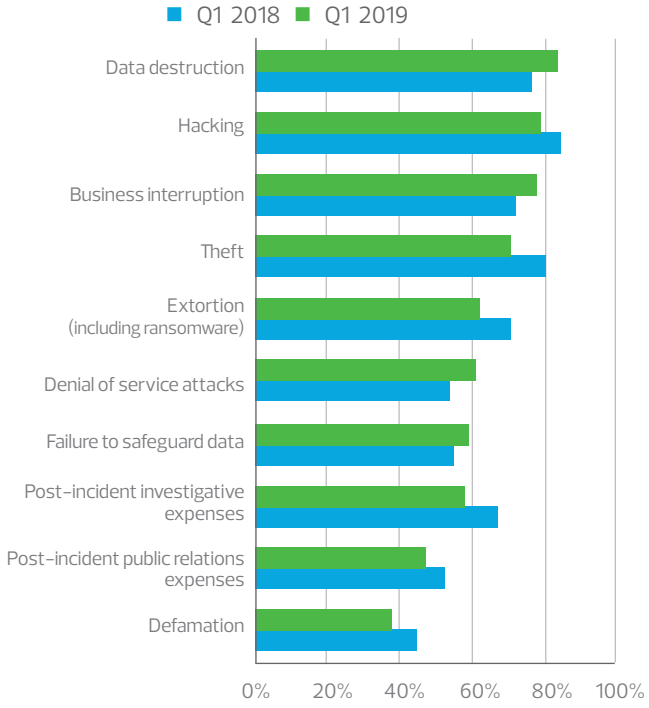



Geopfert sees many common mistakes that come back to haunt organizations. "Make sure your policy covers all the common attack types, including ransoms and losses due to social engineering," he said. "Also, ensure your policy has specific requirements for penetration testing, security monitoring and others, and confirm you are meeting those obligations. If you violate the requirements of the policy, the insurer can claim that the policy is not in effect."

Much like general liability policies, the options for cyber insurance policies are very broad and can be tailored to meet an organization's specific needs. In RSM's survey, middle market executives report that their cyber insurance policies most frequently cover data destruction (83 percent), hacking (78 percent), business interruption (77 percent) and theft (71 percent).

Data breaches are on the rise, and just one incident can cause significant damage to a middle market organization. Cyber insurance policies are an effective tool to limit the consequences of a breach from a financial, operational and reputational perspective.

### Risks or exposures the cyber insurance policy covers

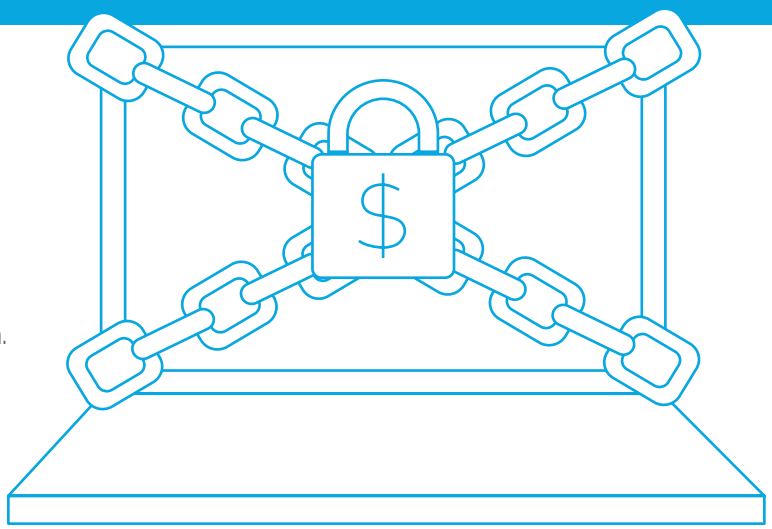



> "Cyber insurance is only as good as the application or questionnaire you fill out. Have a cybersecurity advisor review the application before you submit it."
>
> *– Ken Stasiak, principal, RSM US LLP*

While implementing a policy is important to limit exposure, companies must also remember to periodically evaluate existing policies to account for evolving and emerging risks.

"Cyber insurance is only as good as the application or questionnaire you fill out," said Stasiak. "Having a cybersecurity advisor review the application before you submit it can help confirm that your coverage matches your risks."

# RANSOMWARE ATTACKS



In many ways, 2018 was the year of the lazy hacker, demonstrated by the rise of ransomware attacks on U.S. businesses. Ransomware has evolved from a nuisance to a major threat—a relatively easy attack for hackers, but one with the potential for significant losses to the targeted organization. Media reports often focus on large ransomware attacks that target major cities and multinational companies, but the middle market has also suffered major damage from the ransomware threat.

While traditional "spray and pray" ransomware attacks involving fraudulent emails from fake or compromised accounts may never completely go away, cybercriminals have become much more sophisticated with their methods. Today's attacks take a more targeted approach, seeking out vulnerable networks and systems.

For example, robotic process automation applications are gaining traction within middle market companies to gain efficiency in repetitive business processes. Hackers are now leveraging a similar approach to launch ransomware attacks. Automated systems seek out the low-hanging fruit without a significant amount of effort from the hacker itself.

"If you bet red or black at the roulette table, your chances of winning are 50 percent," Stasiak said. "However, if you add in the 0 and 00, the house will win sometimes. Within your company, you don't have to be 40 percent better at cybersecurity, just enough to tip the odds."

Once a hacker or specific type of malware accesses a network, it attempts to encrypt certain types of files that have a high probability of containing critical data, and then presents a message communicating that files have been encrypted. This message also includes a ransom note with the amount necessary to unlock files before they are destroyed. Targets must decide whether to pay the ransom or attempt to rebuild files and system architecture. Even with backups, that task is time-consuming and may cost more than the ransom itself.

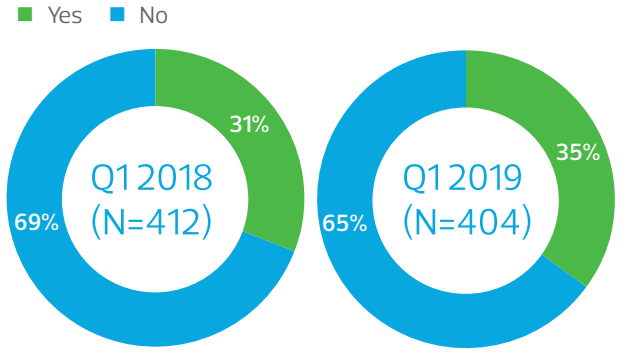
"If you bet red or black at the roulette table, your chances of winning are 50 percent. If you add in the 0 and 00, the house will win sometimes. Within your company, you don't have to be 40 percent better at cybersecurity, just enough to tip the odds."

*— Ken Stasiak, principal, RSM US LLP*

The shift to ransomware is a logical reaction to economic pressures within underground markets. Large data breaches have flooded those markets with an immense amount of data, such as stolen credit cards and identities. Therefore, supply and demand has driven down the value of those stolen goods. Ransomware allows attackers to attack any system or data that is critical to a business, not just specific data types that can be stolen and resold, and then extract significant payment directly from the victim.

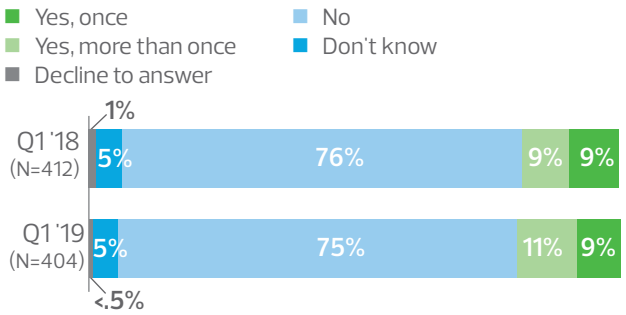
With the growth of ransomware attacks, many middle market organizations either know a peer that has experienced an attack, or been a target themselves in the last year. RSM US MMBI research found that over one-third of middle market executives (35 percent) know someone that has suffered a ransomware attack, compared to 31 percent last year.

## Know anyone that has been the target for ransomware attack



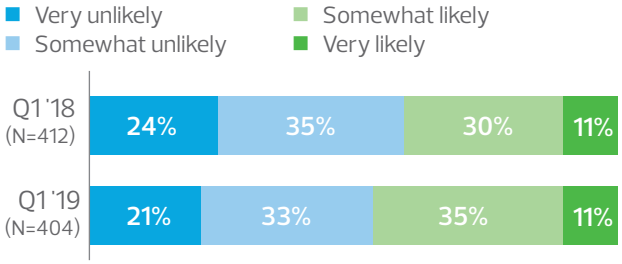

The number of middle market companies that claimed a ransomware attack over the last 12 months has also seen a slight increase. RSM found that 20 percent of executives were affected by a ransomware attack. In fact, 11 percent of organizations reported multiple attacks in this year's survey, up from 9 percent the prior year. Incidence of multiple attacks is significantly larger in middle market companies between $50 million to $1 billion at 15 percent versus just 6 percent at their smaller counterparts.

## Experienced a ransomware attack or demand during the last 12 months




It appears that middle market executives are cognizant of the growing ransomware threat. Forty-six percent of RSM's survey respondents see their organizations as likely targets for a ransomware attack, up 5 percentage points from last year. In addition, more executives at larger middle market organizations see the threat as very likely or somewhat likely than smaller counterparts (52 percent versus 39 percent).

## Likelihood organization is at risk of ransomware attack in next 12 months




Unfortunately, many middle market security frameworks are having trouble keeping up with advances in ransomware attacks. Of organizations that experienced an attack, 50 percent of executives indicated that their existing security and operational controls were not completely successful in preventing or limiting damage. This data represents a 6 percentage point increase from last year's report, consistent with more sophisticated risks to the middle market.

"Security controls are only as effective as their implementation," said Stasiak. "Regularly testing security controls can determine deficiencies before a hacker does."

Any organization in any industry can be at risk for a ransomware attack, as hackers are not necessarily concerned with the size of the company or the data it possesses. With attacks escalating, middle market companies must become more proactive with defense mechanisms. A framework that includes security awareness training for employees, system backups, patch management programs and incident response planning can create a foundation to prevent or address potential attacks.

> "Security controls are only as effective as their implementation. Regularly testing security controls can determine deficiencies before a hacker does."
>
> *— Ken Stasiak, principal, RSM US LLP*

# BUSINESS TAKEOVER THREATS

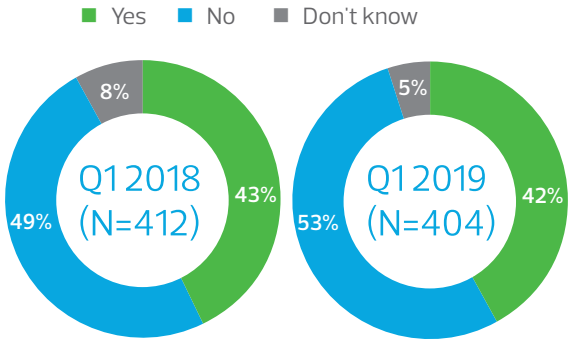
When most organizations think of a cyberattack, high-tech, highly coordinated attack methods typically come to mind. However, sometimes low-tech or even no-tech threats can cause the most harm. Social engineering or employee manipulation attacks fall into this category—simple, yet very dangerous breaches that can be difficult to detect and diagnose.

Social engineering attacks can take many forms. Typically, an attacker contacts an employee directly—by email, phone or even in person—and attempts to trick them into providing access to credentials or sensitive data. Attackers count on employee's desire to help and a lack of security awareness to gain a foothold into an environment and extract as much data as possible.

Phishing remains the most common social engineering strategy, with attackers sending emails that appear legitimate with a link to a malicious website or corrupted attachments. With the amount of personal data available on social media and networking websites, criminals can easily build a profile and initiate communications that appear to be from a superior or other co-worker within the organization.

With the low level of technical skill required, social engineering attacks have become a prevalent threat in the middle market. RSM's MMBI research found that 42 percent of executives indicated 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 metric was roughly identical to last year's data.

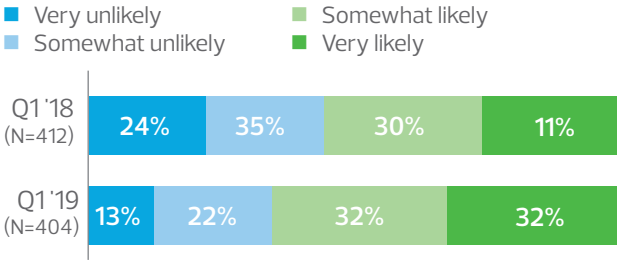
Outside parties attempted to manipulate employees by pretending to be trusted third parties or company executives




However, middle market executives see the social engineering threat growing in the coming year. The RSM study found that 64 percent of respondents say their businesses are likely at risk of an attempt to manipulate employees in the next 12 months, a 9 percentage point increase over last year's data.

"Phishing attacks are like casting a net in the ocean," commented Stasiak. "It's easy to do, and generally yields high returns."

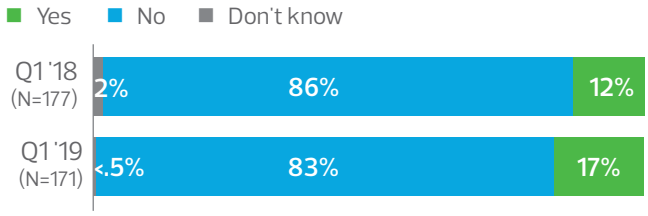
Likelihood organization is at risk of attack by manipulating employees into providing access to business processes in the next 12 months




Criminals who perpetrate social engineering attacks are very persistent, but luckily, most attacks are not successful. Among middle market executives who reported attempts by outside parties to manipulate employees, 83 percent indicated that attempts were not successful. However, executives at larger middle market companies stated that 25 percent of social engineering attacks were successful, and just one successful breach can result in significant consequences.

"We have seen an increase in phishing attacks coupled with vishing over the phone," said Stasiak. "Employees are being scammed via two separate communication methods."

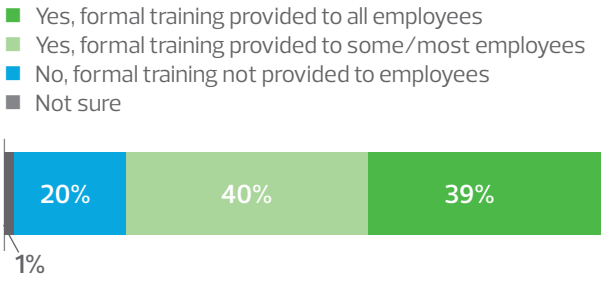
Success of attempts to manipulate employees (N=177)




With social engineering representing such a broad threat, companies must have multiple layers of protections in place. Of organizations in RSM's survey that experienced unsuccessful attacks, 97 percent listed employees not acting on the fraudulent request as a reason for the failed breach. In addition, 58 percent of middle market executives said that secondary controls prevented the completion of an attack, and 43 percent acknowledged system controls that prevented delivery of fraudulent communications or materials to employees.

The majority of middle market executives appear to understand the importance of education in mitigating social engineering threats. In fact, 79 percent of middle market executives 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. These figures reveal an opportunity for the remaining 21 percent of companies to implement training programs.

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




With companies investing more into cybersecurity controls and systems, people are often the weak link within the organization. Middle market companies must be prepared for cutting-edge attack methods, as well as more basic, but still harmful, threats in order to have a comprehensive and effective cybersecurity posture.

"We have seen an increase in phishing attacks coupled with vishing over the phone. Employees are being scammed via two separate communication methods."

*— Ken Stasiak, principal, RSM US LLP*

# PRIVACY PROTECTIONS COMPLIANCE

In addition to a multitude of cybersecurity challenges, middle market organizations now must also be aware of recently enacted data privacy laws and other regulations on the horizon. While organizations have previously focused on how to secure their own data, now they must also comply with regulations that go beyond company data, and govern how personal data—whether from employees, customers or vendors—is processed, stored and collected.

The model for a new wave of international data privacy laws is the EU's General Data Privacy Regulation, which took effect May 25, 2018. The law created new data privacy rules for all companies that transmit, process or hold EU resident data, regardless of whether the companies have European operations. Many companies were slow to develop GDPR-compliant privacy programs, but following several significant enforcement actions, complying with the law now has a high level of urgency.

"Following the effective date of the GDPR on May 25, 2018, many companies opted to take a wait-and-see approach, assuming this to be a distant regulation that would be unlikely to be enforced against U.S. companies," said RSM director Alain Marcuse. "The reality, however, is that enforcement action takes time."

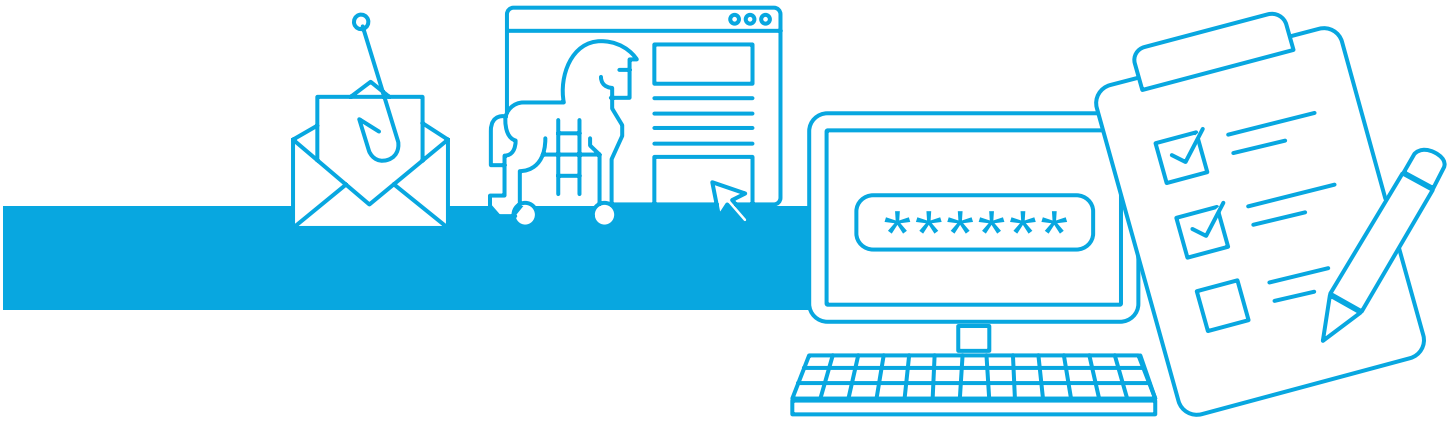
In fact, one of the very first complaints filed on May 25 led to a $57 million fine against Google in January 2019. The penalty was not the result of a data breach, but because of a consumer complaint about Google's handling its data.

"Consumers now have standing to file complaints, and are doing so at a rate of 400 per day," commented Marcuse. "Beyond consumer complaints, U.S. companies—including middle market companies—are increasingly finding that their trading partners are demanding GDPR compliance, and risk losing revenue streams if they can't demonstrate it."

> "Following the effective date of the GDPR, many companies opted to take a wait-and-see approach, assuming this to be a distant regulation that would not likely be enforced against U.S. companies. The reality, however, is that enforcement action takes time."
>
> *— Alain Marcuse, director, RSM US LLP*

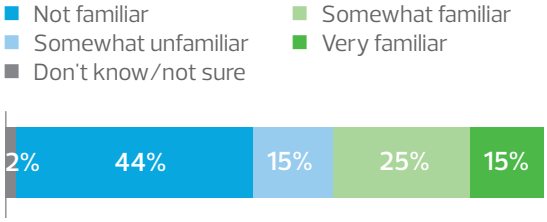
The GDPR has been a successful effort to date, and has inspired similar laws worldwide. In fact, GDPR-style privacy regulations have already been developed by individual U.S. state regulators and others are in the planning stages. The California Consumer Protection Act is scheduled to take effect in 2020, while Massachusetts and Texas already have certain data privacy protections in place. In addition, Congress has held preliminary hearings over similar legislation at the federal level.[5]

5 "Congress is trying to create a federal privacy law," The Economist, accessed April 8, 2019, https://www.economist.com/united-states/2019/02/28/congress-is-trying-to-create-a-federal-privacy-law.



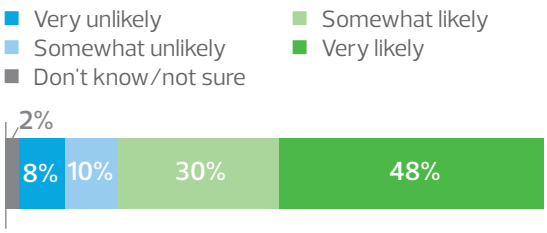

"The GDPR has acted as a trigger for a global wave of privacy regulations that can dwarf the effort companies have put into security," said Marcuse. "Companies need to take this wave seriously, and proactively get their privacy programs developed or updated. The longer they wait, the more difficult the effort will be, and the longer they stay exposed to regulatory and commercial risk."

### Familiarity with requirements of the GDPR (N=404)



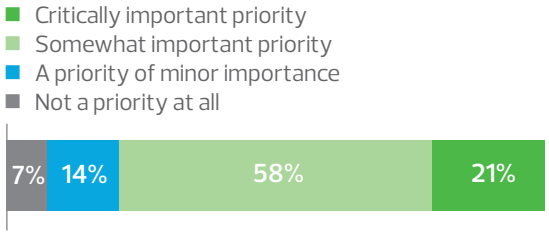

Many middle market companies are required to comply with the GDPR, but only 40 percent of executives in the RSM US Middle Market Business Index research indicated that they are familiar with the requirements of the law. Respondents at larger organizations are more familiar with GDPR requirements than executives at smaller organizations (56 percent versus 27 percent).

### Likelihood organization will have to comply with privacy legislation during the next two years (N=161)




Many executives feel that it is only a matter of time before more extensive data privacy regulations are established in the United States. Among the survey respondents familiar with GDPR regulations, 78 percent 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.

### How much of a priority is preparing for emerging privacy legislation or regulation (N=159)




Regulators worldwide are taking data privacy seriously, imposing significant sanctions for noncompliance. Therefore, many middle market companies are preparing for the future with data privacy in mind. Ninety-three percent 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.

With growing public pressure on companies to protect customer data, middle market organizations can expect more extensive data privacy compliance responsibilities in coming years. Waiting until the last minute to comply with the GDPR, CCPA or any other emerging regulations only increases related expenses and the potential for sanctions. Building familiarity with existing regulations can serve as a helpful foundation to prepare for what is certain to be an active future for data privacy.

A LEGISLATIVE SNAPSHOT FROM THE U.S. CHAMBER OF COMMERCE

# PRIVACY REGULATION
## SPREADS FROM EUROPE TO THE U.S.

Last year marked a watershed for worldwide and domestic privacy regulation. Europe's General Data Protection Regulation, known as GDPR, took full effect; meanwhile, California enacted the nation's first comprehensive privacy law. These regulations foreshadow an effort by legislators on Capitol Hill to consider federal privacy legislation in 2019. Additionally, stakeholders such as the U.S. Chamber of Commerce published model privacy legislation, marking a shift on the part of the business community from supporting self-regulation to promoting federal standards.

On May 25, 2018, the GDPR became fully enforceable. The GDPR recognizes multiple lawful bases for the processing of data such as handling only the information necessary for the performance of a contract, the vital interest of the data subject, and for the public interest. Individuals have the right to know how data controllers are using and sharing data and if that data will be transferred internationally. Additionally, GDPR stipulates that an individual has the rights to a copy of the data from a controller, which is defined as an entity that determines the means and purposes of data processing, as well as to have data about that person deleted. The European law also gives an individual the right to transfer data to a third party, a process known as data portability. Additionally individuals may object to having decisions made about them based upon automated processing. Violations of the GDPR can result in fines of up to 4 percent of a company's annual global revenue.

On June 28, 2018, Governor Jerry Brown signed the California Consumer Privacy Act, the first comprehensive privacy law in the United States. The CCPA requires that businesses provide consumers before or at the point of data collection with the categories of personal information being collected and how that information will be used. California will also require companies, upon verified request, to provide consumers copies of the data. Consumers also have the right to request information about data use and collection. They also enjoy a qualified right of data deletion, and may order a company to stop selling personal information; businesses may also not sell information about individuals 16 and younger without affirmative consent. Companies may not discriminate in terms of pricing, service or quality against consumers who exercise their privacy rights under the CCPA. Violations of the CCPA would subject businesses to civil penalties up to $7,500 per violation, in addition to private lawsuits in the case of data breach involving certain types of personal information.

Currently the State of Washington's legislature is taking up S. 5376, the Washington Privacy Act, which would give consumers the right, upon verified request, to the following: information about data processing, correction of data, deletion of data and restricted processing. Controllers of data must also provide meaningful privacy notices.

On Feb. 13, the U.S. Chamber of Commerce released its own model privacy legislation. This proposed legislation would require that companies larger than small businesses provide consumers, upon verified request, the categories and business purpose of personal information they use and the types of entities with which the business shares that information. Consumers would gain the right to have personal information deleted and not shared with third parties. The Federal Trade Commission generally would enforce the Act and give companies the ability to correct good faith mistakes.

In Congress, several proposals have been introduced. Senators Amy Klobuchar (D-MN) and John Kennedy (R-LA) introduced a privacy bill focused on social media, while Senator Marco Rubio (R-FL) proposed a bill that would grant the FTC online privacy rulemaking authority. Senator Cortez Masto (D-NV) has also proposed a comprehensive privacy law that applies to both online and offline entities. Activity around federal privacy legislation is expected to increase as both the House and Senate Commerce and Senate Judiciary Committees continue to hold regular hearings on data privacy.

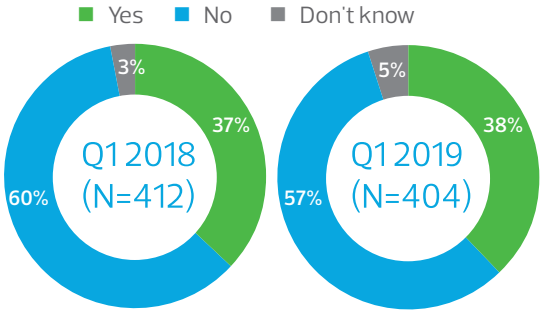
# MIGRATION TO THE CLOUD

As companies grow, they can lose control of their data, not understanding how much information they have and where it resides. In response, many middle market companies are moving data to the cloud for increased efficiency and access, but also greater security. Cloud vendors' economy of scale enables them to implement more extensive security measures and controls that are not typically realistic for middle market companies.

"Before moving to a cloud solution, ensure that you understand the data the cloud provider is storing or accessing," said Stasiak. "This will determine the level of security needed by the provider."

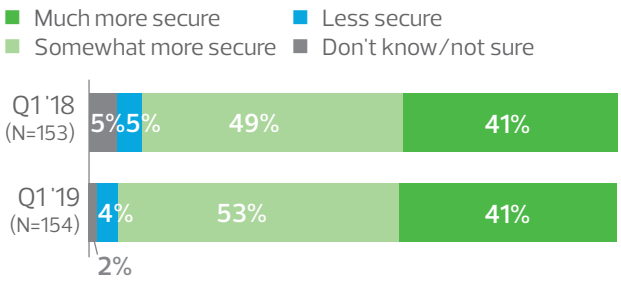
The RSM US Middle Market Business Index data demonstrates the gradual migration of middle market data to the cloud. The survey shows that 38 percent of respondents moved data to the cloud as a result of security concerns in the last 12 months.

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



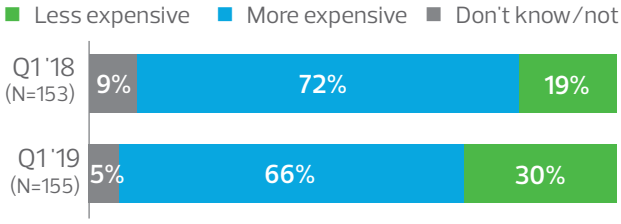

Executives are more comfortable with the decision to move to the cloud, due to a general feeling that the cloud security has improved. Among middle market executives reporting moving data to the cloud for security concerns, 94 percent believe the data residing in the cloud is more secure than in the past.

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




Organizations commonly see cost savings when transitioning data to the cloud, as costs are going down due to saturation in the market. For example, the survey found that 30 percent of middle market executives that moved data to the cloud for security concerns indicated the solution is less expensive, a significant increase from last year's data (19 percent).

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




However, given the saturation in the cloud market, businesses must be careful when choosing potential providers. Companies should undergo a thorough due diligence process on vendors to ensure that solutions are truly secure and the necessary level of access is available. When utilizing a third party, the company that owns the data still retains the responsibility if an incident occurs, and a breach in the cloud can be harder and more expensive to remediate.

Cloud providers should also be a key consideration when selecting cyber insurance. "Ensure that your cyber insurance policy covers breaches at a cloud provider," commented Stasiak.

In addition to the cloud, blockchain solutions are becoming a viable alternative to enhance data security. RSM research found that 22 percent of organizations are pursuing blockchain technology to ensure security or privacy of data. More larger middle market organizations are evaluating blockchain than smaller peers (38 percent versus 10 percent).

Middle market companies now have more options than ever to store data more securely than within on-premise servers. However, a crowded marketplace can also present new challenges. Organizations must be careful when evaluating potential providers to ensure that solutions align with their risk tolerance and business goals.

## Security mavericks to middle market directors:

# BECOME A HARDER TARGET

*The National Association of Corporate Directors, which has a partnership with RSM, recently held a roundtable to discuss cybersecurity risks and challenges.*

Imagine you've spread your prized possessions out on your dining room table. If a burglar manages to make her way past locked doors and windows, she could plunder those items in minutes and disappear back out into the night. You've made her job easy with one layer of defense, no alarm systems and valuables left in plain sight.

However, if you have a safe bolted to the floor, the burglar may get past your basic external defenses, but remain in the dark in an unfamiliar place, trying to hunt for valuables while remaining undetected. Odds are she'll step on that squeaky floorboard or otherwise alert you to her presence. If she does find the safe, she'll struggle to crack the combination, and might even give up trying before being caught.

While comparing a cyber breach to a burglary may seem like a stretch to some, Geopfert says it's an apt metaphor for what a breach looks like at some middle market companies.

In the roundtable discussion, Geopfert noted that people have an inherent understanding of how to protect physical property, but often abandon the same concepts when it comes to securing digital assets. This has led to skyrocketing rates of data breaches within the middle market, which happens to comprise of the majority of American businesses.

### Market-specific risks

Middle market companies often partner with third-party vendors to extend their growth, a move that compounds risks. Both information technology staff and the general counsel's office must track the vendor's compliance with their own security expectations, which can lead to vulnerabilities. In order to mitigate these risks, companies must insist on including protections within contracts that would harden the security stance of their enterprise.

Management should remember that, while moving data to the cloud can enable growth, the softening of security that can occur when working with third parties can lead to chaos when breaches occur. However, organizations have the opportunity to pressure test their security to verify if effective controls are implemented.

"When you ask companies simple questions to verify the protections in place in their systems, their staff oftentimes pause and say, 'You know, we've never verified X, and we're not sure about why we haven't," said Craig Hoffman, a participant in the roundtable and a partner at law firm Baker & Hostetler, describing his experience as a forensic investigator in breaches of midcap companies.

Companies might say they segment their data, which is a common data security best practice, but third parties may not have been called in to independently verify that the segmentation was properly performed, he explained. This lack of assurance creates vulnerabilities that could make or break a company in the event of a breach.

Another roundtable participant noted that boards of mid-cap companies can mitigate the risk of cyberattack by insisting that the company define its risk appetite and security processes.

"A lot of businesses think they understand their business processes, but they really don't," the director said. "They don't document processes, and they rely on prior knowledge. If you can have the self-discipline to document the business process, then you'll have the ability to say, 'How will we definitively know as a board whether or not we lost data based on this diagram?"'

Due to budget constraints, many midmarket companies may choose to invest in a lower tier of service when purchasing certain security and information technology. With limited cost comes limited coverage, however. Returning to Geopfert's metaphor, you would not want to secure your prized possessions in a subpar safe. The same goes for your company's digital assets.

"The second you are small enough to convince yourself that you don't matter, you're the key demographic. However, some companies have turned themselves into exceptionally hard targets in short order because their organizations are that much simpler."

*— Daimon Geopfert, principal, RSM US LLP*

Consider, for instance, the importance of reviewing logs once a breach has occurred. In order to save money, Hoffman pointed out that companies might choose server packages that do not include log maintenance beyond 30 days of coverage. He urged directors to ask their legal teams if contracts have been carefully reviewed to understand the extent of coverage provided. Doing so can help them weigh their coverage against their accepted risk tolerance.

## Play to strengths

The limited size of middle market companies means less surface area to protect—and fewer people to train on security. While the overall target area is larger due to the sheer number of mid-cap companies, individual companies may realize some size-based advantages. "You can't hide on the Internet," Geopfert said. "Hackers quite often aren't looking for anything specific, and because there are so many smaller companies out there, the statistics say they're more vulnerable."

To be sure, the speakers were keen to point out that a smaller footprint means greater speed to strengthening security—and greater opportunity for employees to alert one another when something looks fishy. When one attendee asked what organizations that are smaller and have fewer resources can do to secure their enterprises, Geopfert offered words of reassurance.

"The second you are small enough to convince yourself that you don't matter, you're the key demographic," he said. "However, we have worked with some companies that have turned themselves into exceptionally hard targets in short order because their organizations are that much simpler."

Middle market companies must understand that their organization is indeed a visible target, and that one of their top priorities is to make it harder for cyber thieves to gain entry.

"You can't hide your assets any more than you can hide your house," Geopfert said. "That said, you know where your important things are. Do what you can to lock them down."

-National Association of Corporate Directors
*(A version of this article originally appeared in the September/October 2018 issue of NACD Directorship magazine.)*

# Top of mind cybersecurity concerns in the middle market

We asked about cybersecurity in the first quarter 2019 MMBI topical questions section. It appears that cyber-related themes were among the leading issues for many of the business owners polled. Here is a sampling of cyber-focused responses when executives were asked to describe "a top business concern" for their companies.

"Cybercrime is the biggest problem our business is facing."

"We are facing security risk all the time."

"Taking business from online communication and the risk of fraud."

"Company data sometimes faces risk because of lack of security."

"Security breach incidents."

"Security and technology implementation, integration of it and process for profits and risk."

"Facing security issues and spending a lot of money to protect company data."

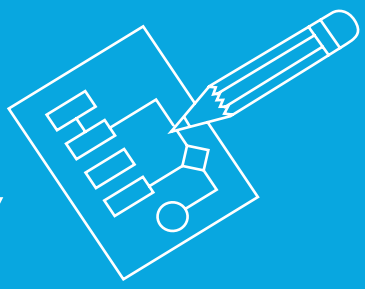
"Security issues. Worrying that our anti-virus and firewalls are always up to date."

"Security and compliance have been our major pain points for quite some time."

"Cybersecurity is a major ongoing issue."

"Financial security electronic risk management."

# METHODOLOGY



## ABOUT THE RSM US MIDDLE MARKET BUSINESS INDEX RESEARCH

The RSM US Middle Market Business Index survey data in the first quarter of 2019 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 first quarter survey was conducted from Jan. 14 to Feb. 1, 2019. Information was collected by phone and online survey from 404 executives, including 257 panel members and a sample of 147 online respondents. Data is weighted by industry.

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

## ABOUT THE NETDILIGENCE® 2018 CYBER CLAIMS STUDY

The 2018 NetDiligence Cyber Claims Study sent requests to 52 individuals at 37 organizations in the United States, Canada and the United Kingdom. Of the cases in the analysis data subset, 1,133 cases represent claims from U.S. organizations, while 10 were from Canada. Additionally, nine cases were from the United Kingdom; three were from Australia; and four claims (one each) were for organizations in China, Germany, Ireland and South Africa. The country was not specified in 42 claims in the data set. This data was provided by 19 individuals representing 17 organizations. The 2018 report also includes data from studies published in 2014 to 2017 as well as 538 cases collected in 2017. It summarizes findings from a sampling of 1,201 submissions each representing a data breach insurance claim.

RSM US LLP is a co-sponsor of the NetDiligence report.

For more information on RSM, please visit **rsmus.com**.
For media inquiries, please contact Terri Andrews, National Public Relations Director, +1 980 233 4710 or terri.andrews@rsmus.com.

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




For more information on the U.S. Chamber of Commerce, please visit **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**