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. Data for the MMBI is gathered through quarterly surveys of the RSM US Middle Market Leadership Council, a panel of 700 middle market executives managed by the Harris Poll. This special edition is a supplement to the first quarter 2018 report.

U.S. CHAMBER OF COMMERCE

RSM

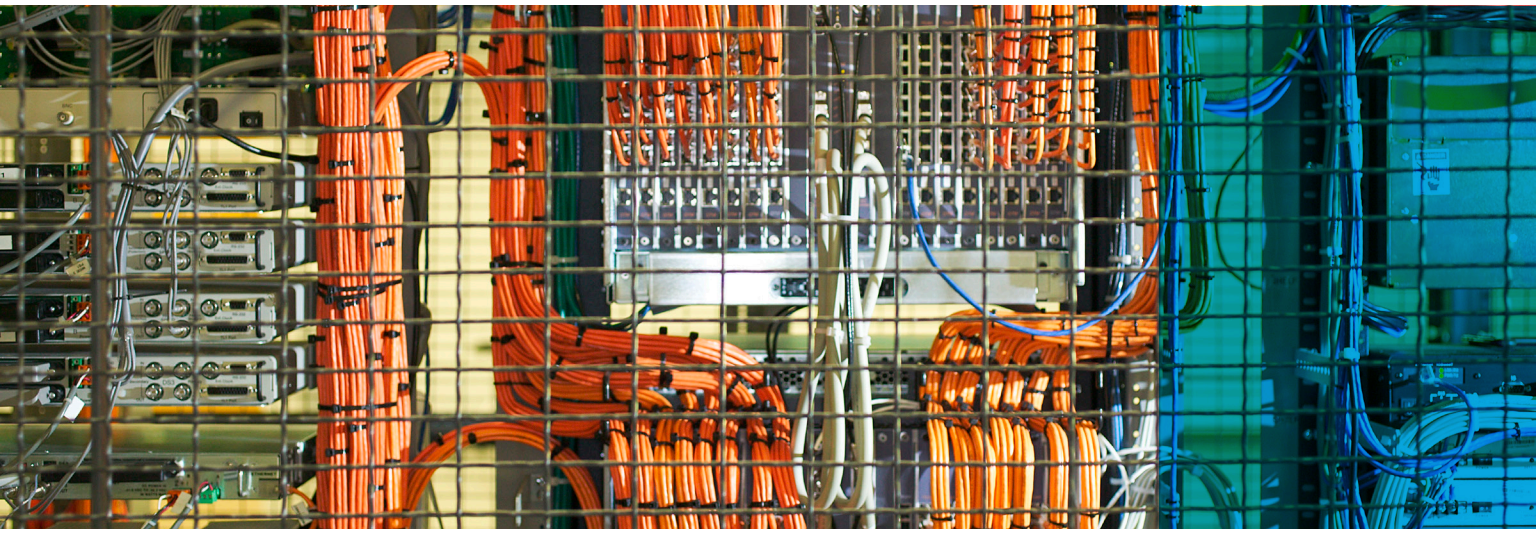
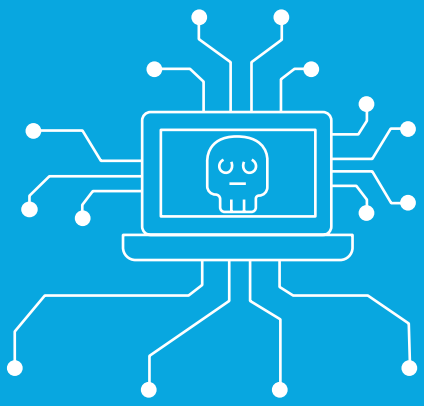


TABLE OF **CONTENTS**



CYBERSECURITY

UNDERSTANDING THE THREAT

Middle market particularly susceptible to cybercrime

The age of big data translates to even bigger risk for businesses of all sizes, but middle market companies are particularly vulnerable.

While widely reported hacks of large corporations such as Equifax and Uber made headlines in 2017, lesser known was the multitude of breaches into midsize businesses, which are increasingly landing in the crosshairs of cybercriminals.

Compared to just three years ago, significantly more middle market companies (13 percent versus 5 percent) contend they experienced data breaches, according to the RSM US Middle Market Business Index.

Bigger middle market businesses, with enough scale to attract cybercriminals but typically lacking the defensive resources of their large-cap rivals, have become attractive targets, according to the data from the responses of some 400 middle market executives.

From ransomware attacks and identity theft to intellectual property risks and privacy concerns associated with the increased use of digital currency, the security of electronic information is set to remain among the biggest challenges facing companies in the 21st century.

There are few signs of crime abatement in the ever-changing cyber landscape. Nearly 50 percent of midsize companies expect they will face unauthorized users attempting to breach their data or systems this year, according to the executives surveyed.

Moreover, despite incidents of rising cybercrime, just half of the businesses surveyed carry cyber insurance policies to protect against internet-based risk. Our study shows that many of those policies may fall short of comprehensive coverage.

Meanwhile, the C-level executives we surveyed may be overly confident in their firms' internal abilities to thwart an attack. Some 93 percent of respondents were confident in their organizations' ability to safeguard customer data. The reality—based on actual incident reports—is proving that confidence may be misguided. While smaller companies were hardest hit last year, midsize companies with annual revenues of $50 million to $300 million accounted for a fifth of cyber incidents, according to NetDiligence®, which produces a yearly report, sponsored by RSM, that tracks cybercrime. Those companies with higher levels of income suffered significantly fewer incidents.

Cybercrime behaves much like a mutable disease, continually evolving, pushing new boundaries, finding vulnerabilities and subsequently exploiting weaknesses. We have developed this report to shed light on some of the important trends related to cyber incidents in the middle market, and the steps that midsize companies can take to mitigate ongoing risk.

INFORMATION AND **DATA SECURITY**

Data is often the most valuable resource for middle market companies, as information can help make more informed decisions and guide organizational strategy. Unfortunately, that information also carries a high value to hackers and other cybercriminals who seek sensitive customer and employee data or intellectual property.

While many middle market organizations consider themselves too small to be a target, data breaches and breach attempts in the sector are on the rise. In many cases, it's not a matter of whether an organization will be breached, but when.

RSM's 2018 first quarter Middle Market Business Index research polled 412 middle market executives about cybersecurity challenges, taking the pulse of the entire segment, and in some cases, providing targeted data for smaller ($10 million to less than $50 million in revenues) and larger ($50 million–$1 billion in revenues) organizations.

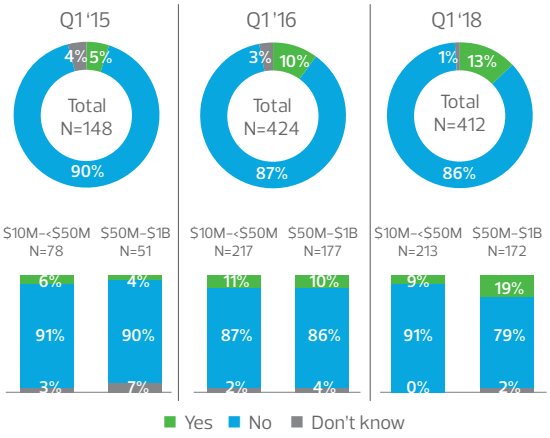
In the survey, executives disclosed that they are experiencing more data breaches. In fact, the number of middle market companies reporting breaches has more than doubled in the last three years, with 13 percent of businesses in 2018 claiming to have endured a data breach, compared to only 5 percent in 2015.

There is no denying that the middle market has become a primary target for hackers. The recent NetDiligence® 2017 Cyber Claims Study found that companies with less than $50 million in revenue accounted for 48 percent of cyber insurance claims from 2014–2017, with another 24 percent from organizations with $50 million–$300 million in revenue. All told, companies with less than $2 billion in revenues represented 88 percent of all reported claims.

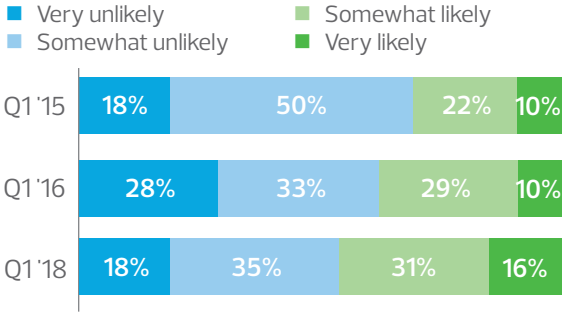
In addition, for the first time since 2015, a plurality (47 percent) of middle market executives indicated an attempt to illegally access their data or systems is "likely"—a significant increase over just two years ago (39 percent). The percentage of respondents claiming that an attempt is "very likely" also surged to 16 percent in the first quarter, compared to 10 percent two years ago.

The costs related to a data breach can be harmful, especially for middle market businesses. According to the NetDiligence study, the average breach cost submitted for cyber insurance claims from 2014–17 was $394,000, with $56,000 the median. Financial costs are often not the only repercussion related to a breach, with regulatory sanctions and reputational damage often following quickly after an incident.

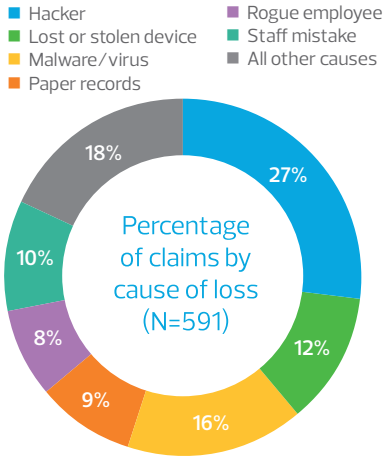
Companies experiencing data breaches in last 12 months



Likelihood unauthorized users will attempt to access data/systems

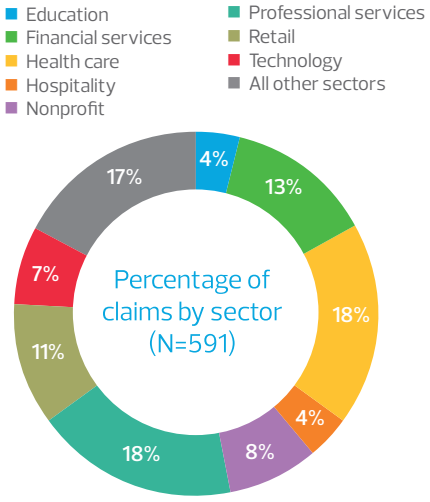


While hackers are the most common source of data and information losses, organizations must also understand the other threats that could result in losses. In the NetDiligence survey, hackers[1] comprised 27 percent of losses, but malware and viruses (16 percent), lost or stolen devices (12 percent), staff mistakes (10 percent), paper records (9 percent) and rogue employees (8 percent) also presented significant threats.



"While hackers represent the single largest external threat, our claims study data shows that insiders are also a major problem," said Mark Greisiger, NetDiligence president. "Rogue employees, trusted vendors, staff mistakes, social engineering, improper handling of patient documents, etc.—these types of insider-driven events account for more than half of all losses."

No industry is immune to data loss or theft. NetDiligence is finding that professional services and health care (18 percent each) experienced the largest number of cyber claims in 2017. Financial services (13 percent) ranked third, followed by retail (11 percent), nonprofit (8 percent) and technology (7 percent).



"It's clear that cyberrisk and losses are occurring in practically every business sector," said Greisiger. "We used to think that most incidents occurred in one of three sectors: health care, retail or financial services. Our data clearly shows that's no longer the case. Simply put, regardless of your business sector, your organization is at risk."

1 In the NetDiligence survey, a hacker is defined as a criminal who manually accesses internal networks and servers in order to access or steal company data or intellectual property.

While threats are rising, and new data security challenges emerge as information continues to gain value, most executives remain confident in their existing data security measures. RSM's research found that 93 percent of middle market companies are confident in their current ability to safeguard sensitive customer data. Despite more breaches being reported and more attempts at illegal data access expected moving forward, executive confidence has risen from 75 percent just three years ago.

This strong confidence in companies' internal security controls and capabilities is likely driven by increased investments to protect information in response to publicized data breaches. RSM found that nearly two-thirds of middle market companies (65 percent) updated security protocols, while 52 percent purchased new or upgraded software and 41 percent updated internal privacy policies.

The average investment is still relatively small. A recent Gartner study found that companies average 5.6 percent of information technology (IT) spending on cybersecurity.[2] The rise of breaches in the sector suggests that companies still have work to do to properly defend themselves.

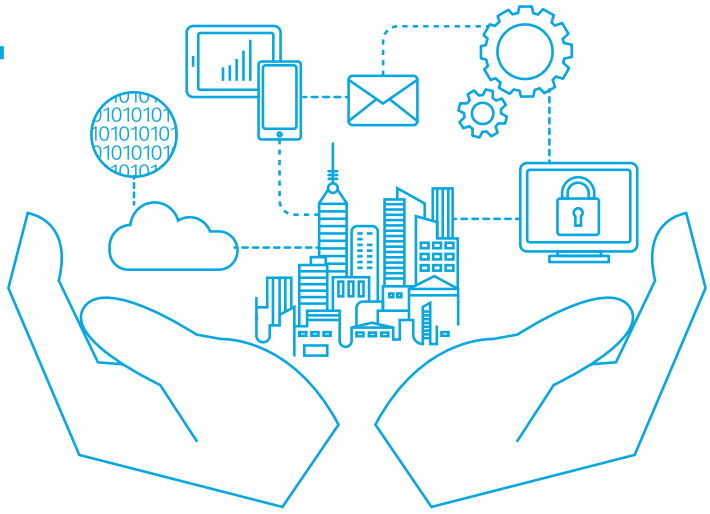
Even with more extensive efforts to curb data breach threats, middle market executives must be careful not to become overconfident and create new vulnerabilities. Criminals are initiating more sophisticated and persistent attacks on internal systems, and can navigate around many protective measures.

"Cyberthreats today resemble a traditional arms race," said RSM Principal and National Security, Privacy and Risk Leader Daimon Geopfert. "The attackers use a method or tool to perpetuate their attacks, and companies respond by implementing new tools and processes to counter the attacks. Those companies feel confident in their ability to handle an incident because of their new resources, but the attackers have since changed tactics and tools thus making their victims vulnerable again."

In summary, the data security challenge is real and growing for middle market companies. The sector has become a major target for data breaches, and organizations might lack the internal resources to understand and detect threats compared to larger counterparts. Companies must place an increased focus on data threats and consider new strategies to protect employee, customer and company data, and preserve confidence in the business and its reputation.

2 "Gartner Says Many Organizations Falsely Equate IT Security Spending With Maturity," Gartner, accessed April 17, 2018.

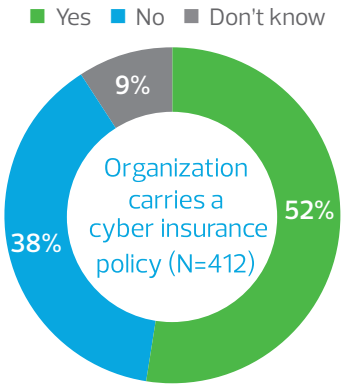
CYBER INSURANCE



When evaluating cyberrisks, middle market companies face various decisions on how to handle risks that correspond to their risk appetites. Cyber liability insurance (CLI) enables organizations to transfer some portion of their cyberrisks, and when coupled with a comprehensive security program, CLI can be very effective. Cyber insurance is often a smart investment to not only protect servers and technology systems, but also to limit risks to a company's sensitive data, finances and reputation.

General liability policies typically exclude cyber insurance coverage. With hacking and data leakage threats looming large to middle market companies, cyber insurance policies bridge the gap to provide liability coverage for data breaches and losses to sensitive customer and company data.

RSM's research found that 52 percent of middle market businesses carry a cyber insurance policy to protect themselves against internet-based risks. Larger organizations[3] tend to invest in policies (58 percent) slightly more than smaller companies (49 percent).



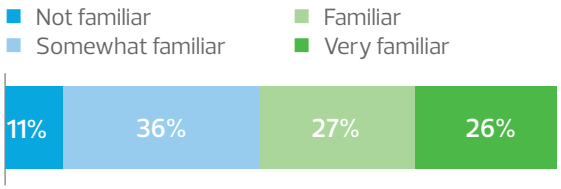
Like general liability insurance, cyber insurance policies can differ, with varying levels of features and protection. Policies can include system repair and data recovery following a breach, as well as the often costly process of notifying customers that their information was exposed—a regulatory requirement in many states and industries.

However, among middle market executives whose companies have cyber insurance policies, many do not understand their level of coverage. RSM's research found that 53 percent indicate familiarity with coverage, while the remaining 47 percent is only somewhat familiar or not at all familiar.

"For many clients, insurance has been the only reason they are still in business. It is steadily becoming more common to encounter events that are an order of magnitude more expensive, and the rise in fines and class-action lawsuits suggests this trend will continue."

— Daimon Geopfert, Principal, RSM US LLP

Familiarity with what organization's cyber insurance policy covers (N=216)

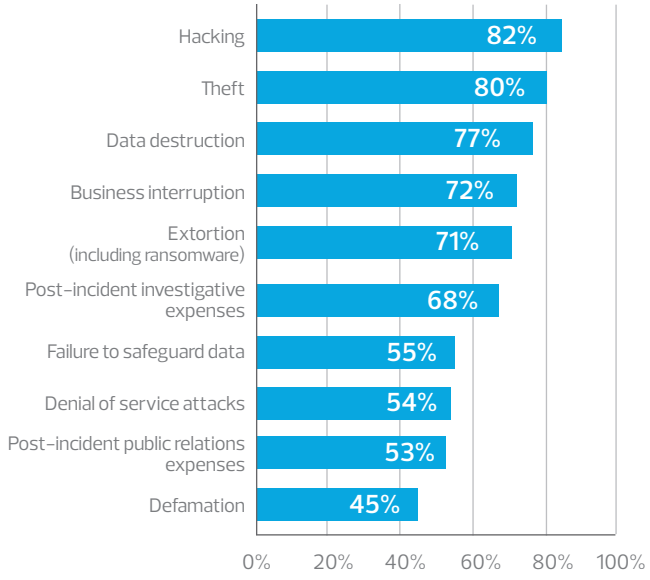


"Our digital forensic teams handle hundreds of client breaches a year, so we have a front-row view of the value of cyber insurance," said Geopfert. "For many clients, insurance has been the only reason they are still in business. It is steadily becoming more common to encounter events that are an order of magnitude more expensive, and the rise in fines and class-action lawsuits suggests this trend will continue."

3 Larger middle market companies have annual revenues of $50 million to $1 billion and smaller companies have annual revenues of $10 million to $50 million.

Executives who claim to understand the details of their cyber insurance policies demonstrated the depth of cyber insurance coverage. Frequently cited risks or exposures covered by cyber insurance policies include hacking (82 percent), theft (80 percent), data destruction (77 percent), business interruption (72 percent), extortion (71 percent) and post-incident investigative expenses (68 percent).

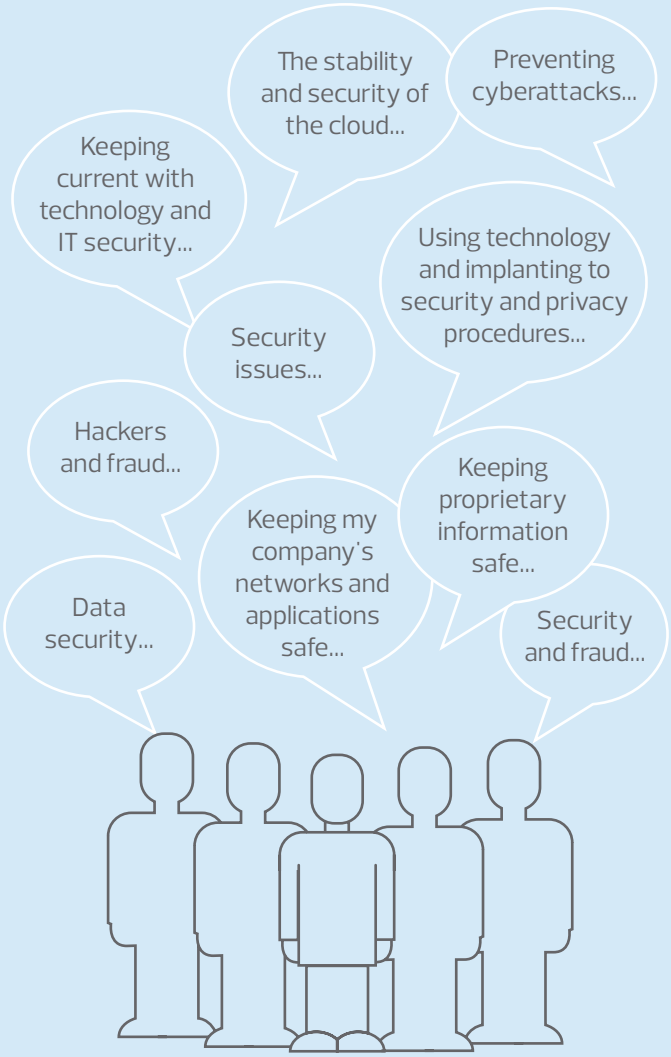
Risks or exposures the cyber insurance policy covers



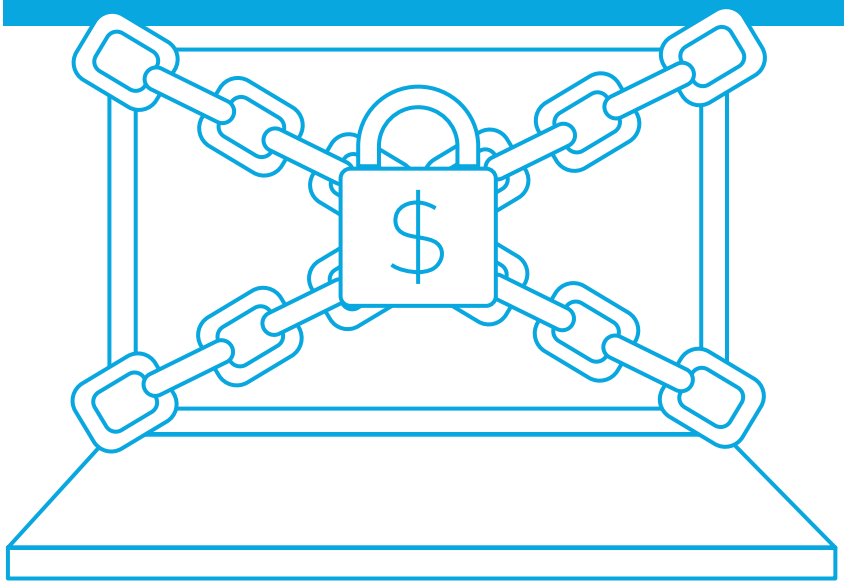
Even a relatively minor data breach can have a significant effect on a middle market organization. Having adequate cyber insurance coverage can help offset the financial, reputational and operational implications of an incident. Amid an environment of evolving threats, leveraging cyber insurance is becoming a smart business strategy, providing peace of mind for the company that breaches will be addressed, and for consumers that their data will be protected.

TOP **SAFETY AND SECURITY CONCERNS** FOR EXECUTIVES

These were among the responses to the RSM survey when executives were asked about the top business problem facing their organization.



RANSOMWARE
BUSINESS ACCOUNT TAKEOVER THREAT



Among data security attacks, ransomware—an attack where hackers hold company data hostage for payment—is a rapidly growing threat due to its ease to deploy and potential to monetize for criminals. While multinational organizations and large government entities garner significant media attention following a ransomware attack, smaller organizations are actually at a more acute risk because of the difference in internal resources.

A ransomware attack often occurs without a distinct target. Ransomware transcends boundaries between company size and industry; hackers deploying this tactic don't care about the data, they care about company operations. So, in essence, the smaller a company is, and how much data it holds, has no bearing on the amount of ransom (typically in bitcoin) the company is required to pay for recovery.

"Ransomware continues to be distributed through traditional means such as fake or compromised email accounts, but we are also seeing a rise in alternative methods of deployment."

— Daimon Geopfert, Principal, RSM US LLP

An attack typically spreads through email campaigns initiated by hackers, with victims coming to the attacker when users—including unsuspecting employees—click on a link to a malicious or compromised website, or open a corrupt attachment.

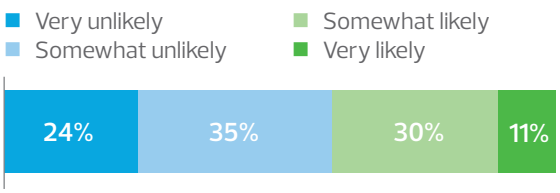
Once executed, a ransomware attack locks a user's computer screen and presents a message communicating that files have been encrypted. That message also includes a ransom note, detailing the amount necessary to unlock files before they are destroyed. Victims face a critical decision—whether to pay the ransom or attempt to remediate the attack and risk losing valuable data. Meanwhile, the ransom amount often increases as the deadline approaches.

"Ransomware continues to be distributed through traditional means such as fake or compromised email accounts, but we are also seeing a rise in alternative methods of deployment," said Geopfert. "As an example, certain hacking crews will breach an organization's environment via traditional means, move through the network as they would during a normal data breach, find the organization's most sensitive systems, and manually deploy the ransomware. The first indicator to the organization that something might be wrong is when their most critical systems suddenly become nonresponsive."

Through personal and peer experiences, many middle market executives understand the severity of ransomware threats. The RSM US Middle Market Business Index research found that nearly a third (31 percent) of executives know someone in another organization that has been the target of a ransomware attack.

Underscoring how pervasive the threat has become, RSM also found that 41 percent of middle market executives see their organizations as likely targets for a ransomware attack. In addition, more than twice as many executives at larger organizations (15 percent)[4] see the ransomware threat as very likely than those at smaller companies (7 percent).

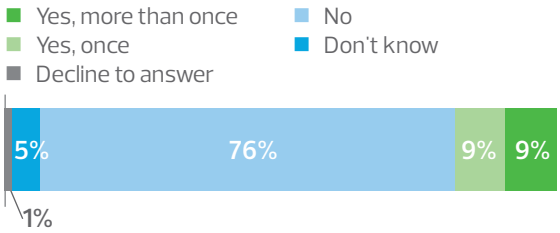
Likelihood organization is at risk of ransomware attack in next 12 months (N=412)



4 Larger middle market companies have annual revenues of $50 million to $1 billion and smaller companies have annual revenues of $10 million to $50 million.

Given the frequency of ransomware attacks, it's no surprise that many middle market organizations experienced the threat first hand in the last year. In fact, 18 percent of middle market executives claimed a ransomware attack or demand during the last 12 months, with 9 percent of companies suffering more than one attack.

Experienced a ransomware attack or demand during the last 12 months (N=412)



Unfortunately, while the ransomware threat increases, protective measures at middle market companies may not be keeping pace. RSM's research found that among breached organizations, 44 percent indicated that existing security and operational controls were not completely successful in dealing with ransomware attacks.

Despite ransomware's growth, many middle market organizations may not understand how a threat manifests itself or the best way to address it. Implementing more effective defense measures including security awareness training, system backups, patch management and incident response planning can help to prevent attacks and respond to incidents.

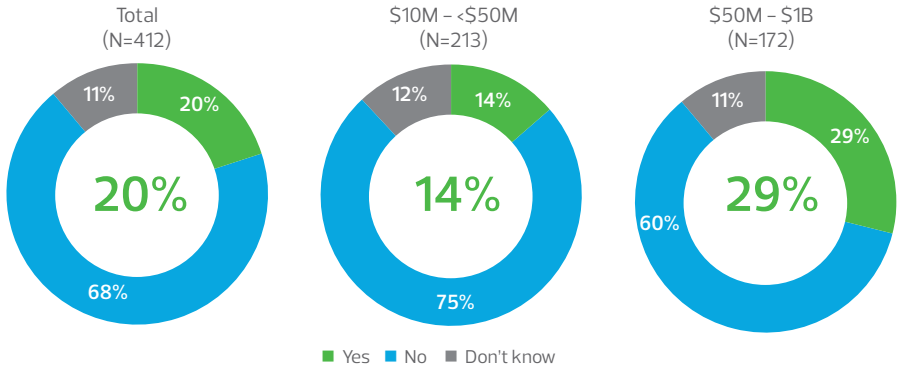
PRIVACY PROTECTIONS COMPLIANCE

As data breaches become more frequent, and threats become more severe, several regulatory bodies are establishing new privacy guidelines to protect sensitive consumer data. One recent example is the European Union's (EU) General Data Protection Regulation (GDPR), which was adopted in April 2016 with enforcement slated to begin on May 25, 2018.

EU privacy regulations are considered to be some of the toughest in the world, and GDPR is no different. All organizations that hold, transmit or process EU resident data must comply with GDPR guidelines, regardless of whether they actually have operations in the EU. Therefore, many U.S.-based middle market companies that possess EU-resident data may not understand that they are subject to GDPR requirements.

Of the executives in RSM's Middle Market Leadership Council representing U.S.-based companies, the 2018 first quarter survey found that only 20 percent of these middle market organizations indicated that GDPR is relevant to their companies. Furthermore, larger midsize businesses (29 percent) are significantly more likely to claim GDPR relevance than smaller organizations (14 percent).

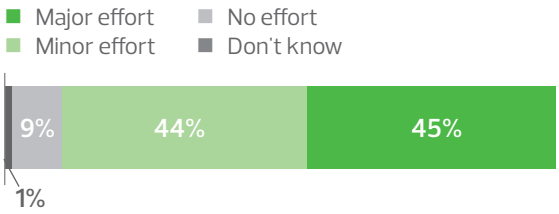
Compliance with GDPR relevant to organization



"While many executives have been dismissive of the impact of GDPR on their organization, they may be ignoring a very significant warning in a way that will cause significant pain later."

– Daimon Geopfert, Principal, RSM US LLP

Level of effort required to comply with GDPR (N=84)



In addition, in companies where GDPR is seen as relevant, executives are divided on the degree of effort required for compliance. RSM found that 45 percent of middle market executives consider GDPR compliance a major effort, while 44 percent believe it is a minor effort.

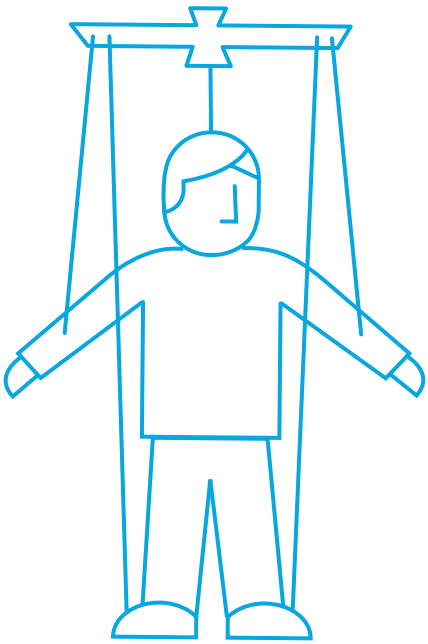
Many organizations underestimate how much EU data they hold, and therefore may not understand the legislation's potential effect. With recent technology advances in digital communication, consumer data can be collected in many ways, including website forms, email systems, social media, mobile platforms and many other business applications. In addition, the GDPR definition of "private data" is much broader than U.S. regulations, including information such as geo-location data, browser cookies, biometric data or any other information that could identify an EU individual.

GDPR has raised the bar for protecting consumer information, and requires tracking of EU personal data from collection to disposal. However, GDPR can also become a business opportunity, with data privacy serving as a competitive differentiator and creating a blueprint to address additional new privacy laws.

Noncompliance with GDPR can result in significant financial penalties, up to 4 percent of global revenue or 20 million euro, whichever is greater. Middle market companies must be prepared, as enforcement actions are expected against the sector first to establish a foundation for pursuing penalties against larger companies.

"While many executives have been dismissive of the impact of GDPR on their organization, they may be ignoring a very significant warning in a way that will cause significant pain later," said Geopfert. "GDPR is an indicator of the very likely course of upcoming privacy laws in the United States, as well as other international locations. Organizations would be well served to start implementing GDPR-style processes around data privacy, consent and "right to be forgotten" so that when such laws inevitably come to the United States or regulatory agencies, organizations can avoid the perspective of having to deploy such controls in a compressed timeline."

SOCIAL ENGINEERING



"The implementation of specific technical controls in conjunction with awareness, should be a focus for organizations. Don't rely on one control or technique, since most attacks evolve very quickly."

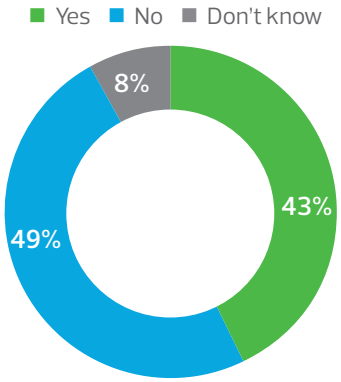
— Ken Stasiak, Principal, RSM US LLP

While many cyberattacks are the result of high-tech hacking attempts, some threats are much simpler, but just as dangerous. Social engineering or employee manipulation attacks are designed to trick employees into granting access to systems or divulging information that can help attackers access sensitive company or customer data.

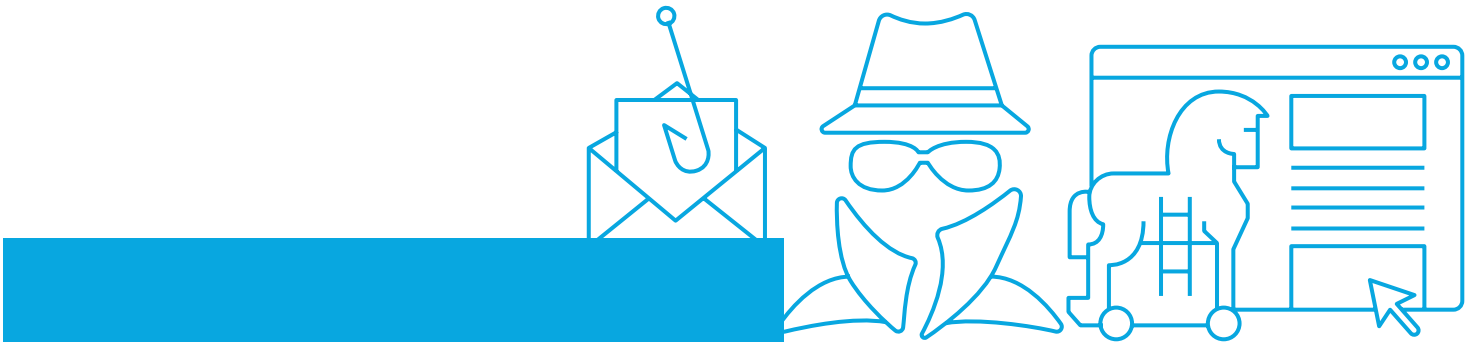
Social engineering attacks can come in many forms. For example, an attack can be initiated via telephone, with an attacker posing as a member of the organization, a customer or a vendor and attempting to gain computer or security credentials. Criminals can also mine employee social media profiles for information that can compromise IT security or trick employees into granting access to systems or providing key information through sophisticated email campaigns.

Social engineering is a particularly harmful threat to middle market companies because it can attack all three layers of defense: personnel, physical and cyber. The most common social engineering strategy involves phishing, which is a combination of personnel and cyberattacks. In some cases, a social engineering attack can be as simple as someone walking into a business and attempting to breach security protocols. Attackers may leave a USB drive that can infect a computer, or again, pose as a customer or IT vendor with the goal of stealing data.

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

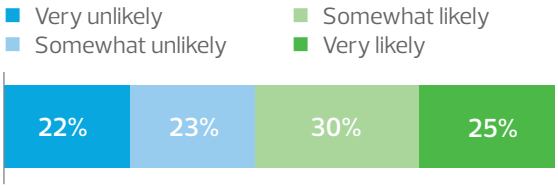


With the relatively low technical experience necessary to launch a social engineering attack, threats have become widespread in the middle market. RSM US Middle Market Business Index research found that 43 percent of executives indicated that outside parties



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.

Likelihood organization is at risk of attack by manipulating employees into providing business processes in the next 12 months (N=412)

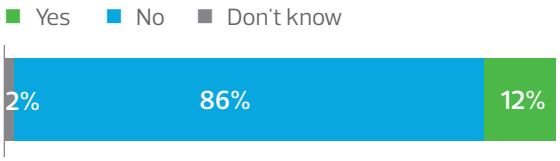


"The first line of defense in many instances is people. Awareness and cultural changes can go a long way in reducing the likelihood of a ransomware attack," said Ken Stasiak, RSM principal. "The implementation of specific technical controls in conjunction with awareness, should be a focus for organizations. Don't rely on one control or technique, since most attacks evolve very quickly."

Executives expect the social engineering threat to continue over the next year. RSM research found that 55 percent of middle market executives say their business is likely at risk to an attempt to manipulate employees in the next 12 months.

Luckily, most attacks are not successful, but just one breach can cause significant damage. Of companies reporting attempts by outside parties to manipulate systems, survey data showed that 86 percent were ultimately not successful.

Success of attempts to manipulate employees (N=177)



With employee manipulation and social engineering presenting such varied and diverse attack methods, middle market companies are employing several strategies to address the threat. The reason cited most frequently (91 percent) in RSM's survey for why attacks were unsuccessful was that employees did not act on the fraudulent request. In addition, 63 percent of middle market executives said that secondary controls prevented completion of an attack and 40 percent pointed to systems controls that prevented fraudulent communications or materials from reaching employees.

While middle market companies must be prepared for high-tech hacking strategies, they also must be aware of employee manipulation and social engineering attacks that often take the form of low-tech or even no-tech efforts.

CYBERSECURITY KEY CONSIDERATIONS

FOR MIDDLE MARKET BUSINESSES

Middle market organizations must evaluate several important issues to address their potential cyber vulnerabilities.

- **Third-party vendor management:** This area is often overlooked, but many third parties store, process, access and transmit potentially sensitive data. Therefore, companies need to make sure that this information is protected when using third parties, such as cloud providers.
- **Identify and access management (IAM):** Companies should invest in technology to secure their applications and systems by leveraging centralized single sign-in and two-factor authentication (such as a username and password, but then also token or text message to a smart phone).
- **Vulnerability management program (VMP):** Organizations should conduct regular testing for known vulnerabilities, for both external (internet) and internal environments. Developing and implementing a program will help ensure that identified vulnerabilities are mitigated in a timely manner.
- **Culture and awareness:** Employee awareness of security-related issues can have a significant impact on the overall security program. By implementing a proactive security awareness campaign in conjunction with periodic phishing tests, companies can help ensure that end users are actively aware of the latest threats.
- **Benchmarking:** Conducting annual risk assessments can provide visibility into an organization's overall risk posture. Benchmarking results year over year and comparing the results to industry averages can provide context to risk appetite developed by senior leadership.
- **Compliance:** Companies should be aware of the various compliance regulations they are required to adhere to. In addition, once they trip the middle market threshold, companies will likely face multiple additional regulations they need to comply with, and they should therefore consider cross-compliance mapping.
- **Incident response planning:** As companies start to develop a larger footprint, their data breach risks will likely increase. In addition, with a larger staff, the need for formal processes is critical so employees understand what to do and are prepared to respond to a breach, both from a technical standpoint as well as a reputational perspective.
- **Cyber liability insurance (CLI):** The ability to transfer some portion of risk is advantageous to middle market companies. Keep in mind when renewing or looking to purchase a CLI policy, the aforementioned focus areas must be addressed. Failure to have an awareness program or an incident response program, etc., may cause premiums to increase or, in many instances, be contingent on having processes in place prior to a claim.
- **Cybersecurity steering committee:** This group can provide a platform to have open discussions surrounding cyberrisks. The committee should include a variety of individuals, including audit, legal, human resources, IT, business owners and cybersecurity resources. The primary objective is to establish a risk appetite and provide overall business guidance on risk decisions.

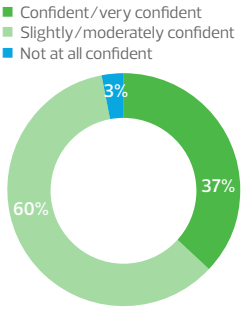
BOARDS ARE LESS CONFIDENT ABOUT CYBERRISK PREPAREDNESS

Thirty-seven percent of board respondents to a recent NACD survey[5] feel confident or very confident that their company is properly secured against a cyberattack, compared to 42 percent last year. A slightly higher percent (49 percent) is confident or very confident in the ability of management to address cyberrisk. The lack of board confidence in their ability to control cyberrisk may be driven by the fact existing defense systems quickly become obsolete when cyberthreats mutate and companies adopt new technologies.

This year's survey findings suggest that boards are gradually increasing their understanding of cybersecurity, which may also explain their increased skepticism of management's efforts. Boards are now more informed and more prepared to challenge the effectiveness of the companies' cybersecurity programs. In 2015, 22 percent of directors reported that their boards had no or very little knowledge of cyberrisk. That figure dropped to 15 percent this year.

More than one-fifth of directors (22 percent) expressed dissatisfaction with the quality of cyberrisk information provided to the board by management. Of those "dissatisfied" or "very dissatisfied" with this information, most indicate that the information they receive doesn't provide enough transparency into problems (44 percent) or doesn't allow for effective internal and external benchmarking (41 percent).

How confident are you that your company is properly secured against a cyberattack?



5 2017-2018 Public Company Governance Survey, National Association of Corporate Directors

"THE IMPERATIVE FOR BOARDROOMS TO CONDUCT SOUND CYBERRISK OVERSIGHT IS HERE TO STAY—IN THE BOARDROOM AND IN THE HALLS OF LEGISLATION. LUCKILY, RESOURCES ABOUND FOR CORPORATE DIRECTORS TO GET UP TO SPEED ON WHAT THEIR COMPANIES NEED TO KNOW AND DISCLOSE WHILE AWAITING REGULATIONS AND RULEMAKING ABOUT CYBERRISK OVERSIGHT."

Peter R. Gleason, President and CEO
National Association of Corporate Directors

TAKE PROACTIVE MEASURES WITH AVAILABLE GOVERNMENT RESOURCES

By Vincent Voci
U.S. Chamber of Commerce

The U.S. Chamber of Commerce recommends reaching out to local federal law enforcement and building relationships prior to incidents. The Department of Justice has trained attorneys in its U.S. Attorney offices as specialists in cybercrime investigations. It also offers voluntary cyber incident guidance for organizations.

We encourage midsize businesses in states and municipalities that don't have an FBI or Secret Service field office, or an office of the U.S. Attorney, to reach out to state and local law enforcement. They should inquire about law enforcement's capabilities and expertise in cybercrime investigations. In addition, the Secret Service operates the National Cyber Forensics Institute (NCFI) in Hoover, Alabama. The Institute trains state and local law enforcement, prosecutors and judges on cybercrime. If your jurisdiction doesn't have sufficient local knowledge, ask officials to consider sending a representative to the NCFI for training.

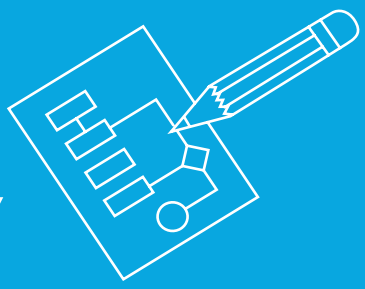
Finally, the Department of Homeland Security is significantly expanding its Cybersecurity Advisor (CSA) program across the country. CSAs offer assistance to help prepare and protect private sector entities from cyber threats by promoting cybersecurity preparedness, risk mitigation and incident response capabilities.

Ultimately, assistance is available for businesses of all sizes and sectors. State or local chambers of commerce resources can help organizations navigate the web of three-letter agencies to help improve risk management and incident response plans. However, at the end of the day, it's up to individuals and organizations to manage their own cyber risk.

Vincent Voci is senior policy manager for cyber intelligence and security with the U.S. Chamber of Commerce. To read a full Q&A with Voci about government regulation regarding cyber issues, please visit rsmus.com.

U.S. CHAMBER OF COMMERCE

METHODOLOGY



ABOUT THE RSM US MIDDLE MARKET BUSINESS INDEX RESEARCH

The RSM US Middle Market Business Index survey data in the first quarter of 2018 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. 12 to Feb. 5, 2018. Information was collected by phone and online survey from 412 executives, including 277 panel members and a sample of 135 online respondents. Data are weighted by industry.

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

ABOUT THE NETDILIGENCE® 2017 CYBER CLAIMS STUDY

NetDiligence 2017 Cyber Claims Study sent requests to 93 individuals at 73 organizations in the United States and Canada. Of the cases in the analysis data subset, 582 cases represent claims from U.S. organizations, while two were from Canada. Additionally, four cases were from the United Kingdom, and two were from Australia. These data were provided by 17 individuals representing 16 organizations. The 2017 report also includes data from studies published in 2014 to 2016 as well as 354 cases collected in 2017. It summarizes findings from a sampling of 2,411 submissions each representing a data breach insurance claim. Those incidents were further culled to 591 relevant events, a large increase over the prior year.

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

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.

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