VASQUEZ
+ COMPANY LLP

Insights for Smarter Decisions

As a member of the RSM US Alliance, we would like to share the following with you.

Cybersecurity considerations and trends for boards and audit commmittees

LOCALLY OWNED. NATIONALLY AFFILIATED. GLOBALLY CONNECTED.

An independently owned member
RSM US Alliance
RSM

Vasquez & Company is a proud member of the RSM US Alliance, a premier affiliation of independent accounting and consulting firms in the United States. RSM US Alliance provides our firm with access to resources of RSM US LLP, the leading provider of audit, tax and consulting services focused on the middle market. RSM US LLP is a licensed CPA firm and the U.S. member of RSM International, a global network of independent audit, tax and consulting firms with more than 43,000 people in over 120 countries.

Our membership in RSM US Alliance has elevated our capabilities in the marketplace, helping to differentiate our firm from the competition while allowing us to maintain our independence and entrepreneurial culture. We have access to a valuable peer network of like-sized firms as well as a broad range of tools, expertise and technical resources.

Los Angeles
+1 213.873.1700

Sacramento
+1 916.503.3269

San Diego
+1 619-254-6605

Manila
+1 213.873.1720

For more information:
solutions@vasquezcpa.com

CYBERSECURITY

CONSIDERATIONS AND TRENDS FOR BOARDS AND AUDIT COMMITTEES

An abridged version of the RSM US Middle Market Business Index Cybersecurity Special Report

2022

Scan here for additional board insights from RSM

RSM

EXECUTIVE SUMMARY

Moving in the **right direction**

Reported breaches drop, but significant cybersecurity concerns persist

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

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

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

REPUTATIONAL RISK

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

NONPROFIT EXECUTIVE

Business leaders provided insight into the evolution of their cybersecurity approaches in a 2022 first quarter RSM US Middle Market Business Index survey. The survey polled 402 senior executives at middle market companies about their cybersecurity and data privacy challenges, detailing the frequency and severity of attacks, and ongoing concerns, while providing a glimpse into how the largest segment of the U.S. economy is implementing controls and strategies to address security threats and fight back against cybercriminals. In many cases, survey research provides specific data for smaller ($10 million to less than $50 million in revenue) and larger ($50 million to $1 billion in revenue) middle market organizations.

22% of MMBI survey respondents claimed their company experienced a data breach in the last year

According to the MMBI data, 22% of executives claimed that their company experienced a data breach in the last year, representing a sizable drop from 28% in last year's survey. Larger organizations were most at risk once again (30%) compared to smaller counterparts (12%), but both showed a decrease in attacks.

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

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

—Matthew Eggers, Vice President of Cybersecurity Policy, U.S. Chamber of Commerce

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

The data privacy landscape continues to evolve in the United States, with constant dialogue about who should collect and possess sensitive data, and how it should be stored. The discussion is no longer just about how information is secured but why organizations need that data in the first place. The European Union's General Data Protection Regulation, known as GDPR, was a trailblazing piece of legislation that went into effect in 2018 and has served as a blueprint for data privacy standards worldwide.

THE DREADED CALL

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

PETROLEUM COMPANY EXECUTIVE

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

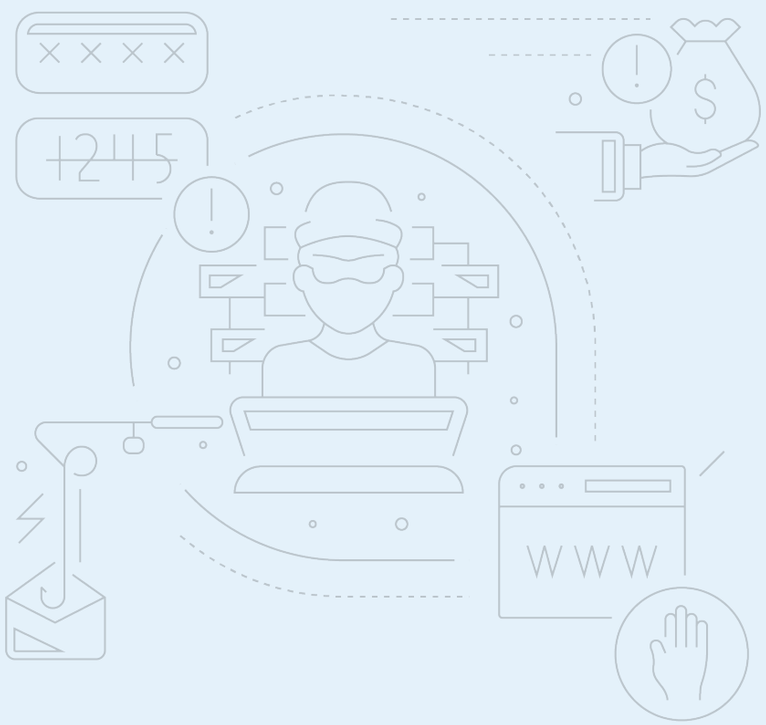
A MOVING TARGET

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

MANUFACTURING EXECUTIVE

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

Organizations face an increasingly volatile cybersecurity environment, with threats coming from more directions than ever before and more skilled criminals targeting the segment. To help ensure effective strategies and controls are in place, companies must take advantage of benchmarking opportunities and learn from the experiences of their peers. RSM has developed this report to provide relevant middle market cybersecurity insights and data privacy trends, as well as to outline tactics organizations can utilize to strengthen security and privacy programs.



Cybersecurity governance and **the board's role**

Proposed SEC rules seek to address risk management gaps across the enterprise

The U.S. Securities and Exchange Commission has proposed amendments to its cybersecurity rules for public companies, aiming to strengthen cybersecurity oversight, governance and incident disclosure. The proposed rules would enhance cybersecurity protocols and require some boards to make structural and cultural changes to address governance gaps and vulnerabilities.

A governance gap between boards and cybersecurity leadership

Similar to the Cyber Incident Reporting for Critical Infrastructure Act of 2022, or CIRCIA, the proposed amendments seek to bridge the common disconnect between boards and cybersecurity leadership. While boards are typically composed of seasoned business leaders, most members lack cybersecurity expertise. Although it is increasingly common for an organization's chief information security officer to brief the board on a quarterly basis, the CISO often reports concerns from a technical perspective that members may not completely understand, let alone know how to evaluate in the context of other corporate governance needs.

In addition, board communication is often limited to affirming technologies previously implemented or reviewing key performance indicators on issues already addressed—while downplaying potential risk to organizational assets. These communication practices can lead members to ask the wrong questions and make ineffective requests and recommendations, exacerbating risks to the business.

"To close this gap, boards must increase their oversight and develop a governance culture which elevates cybersecurity throughout the enterprise and treats it like any other business risk," said Rod Hackman, a member of the board of directors of an SEC-reporting company who leads the board's cybersecurity oversight function. "Until the board and CISO meet in the middle and begin to speak the language of business, and understand cybersecurity as a business risk, effective governance will continue to suffer."

Boards must also understand that other legislation, such as CIRCIA, may have disclosure requirements that overlap the SEC rules—creating conflicting reporting directives that will require resolution.

Practical actions to close the gap

To ensure cybersecurity is a priority for both your board and your management team, communication between the groups must be focused and transparent. Boards should reject the preconceived notion that cybersecurity is too difficult to deal with. According to Hackman, "The first step toward better governance is to engage management, and likely outside advisors, to arrive at a common understanding of how the business works by identifying and mapping all operational and support elements of the business, both internal and external. What are the most important assets, and how do they interact? What threatens them? How will the business respond if threats are realized?"

Cyberthreats affect a complex array of organizational assets that include:

- Data, both structured and unstructured
- Processes, particularly those that contribute to customer experience
- Safety of employees, products and in some cases, customers
- Availability of products and services

To evaluate and address the risks to those assets, a business must have the following in place:

- Process flows for financial compliance
- Business capability models as a basis for broad technological change
- Asset registries for compliance
- Network topologies to support IT management activities

Under the proposed SEC rules, determining the disclosure requirements of a cybersecurity incident will present new challenges, including:

- Establishing materiality of the cyber incident to determine if disclosure is warranted
- Getting a clear understanding of what information will be disclosed and to whom
- Ascertaining if critical company data was improperly accessed, stolen or altered in any way
- Having appropriate expertise on the company board to provide oversight

Mapping cyber risk to organizational assets greatly enhances a board's ability to oversee cybersecurity efforts and helps assure members that investments in that area are effective and align with business objectives.

Steps your board can take to address gaps in communication and governance within your organization include:

Determine organizational perceptions of cybersecurity.
Board members should gather information to assess whether cybersecurity is a shared objective among executive management rather than the sole province of a security or IT department. A board should also understand on what basis management determines the resiliency and security of the organization's assets.

Obtain a full understanding of your organizational assets.
Board members should request a consolidation and summary of organizational assets from management, assessed by business impact and reconciled to security control/framework(s). This information will help the board and management develop a common understanding of cybersecurity, provide both groups with insight into the organization and its underlying technology, and promote a sense of ownership by all. The potential cost of misunderstanding the risk environment compels a high level of visibility and transparency.

Gain clarity on cyber disclosure requirements for your organization.
Board members should understand and challenge management's procedures for assessing both the materiality of a cyber incident and whether it requires disclosure within a prescribed time frame. Both groups should understand the competing disclosure requirements of multiple regulatory authorities and the risk of disclosing inaccurate information.

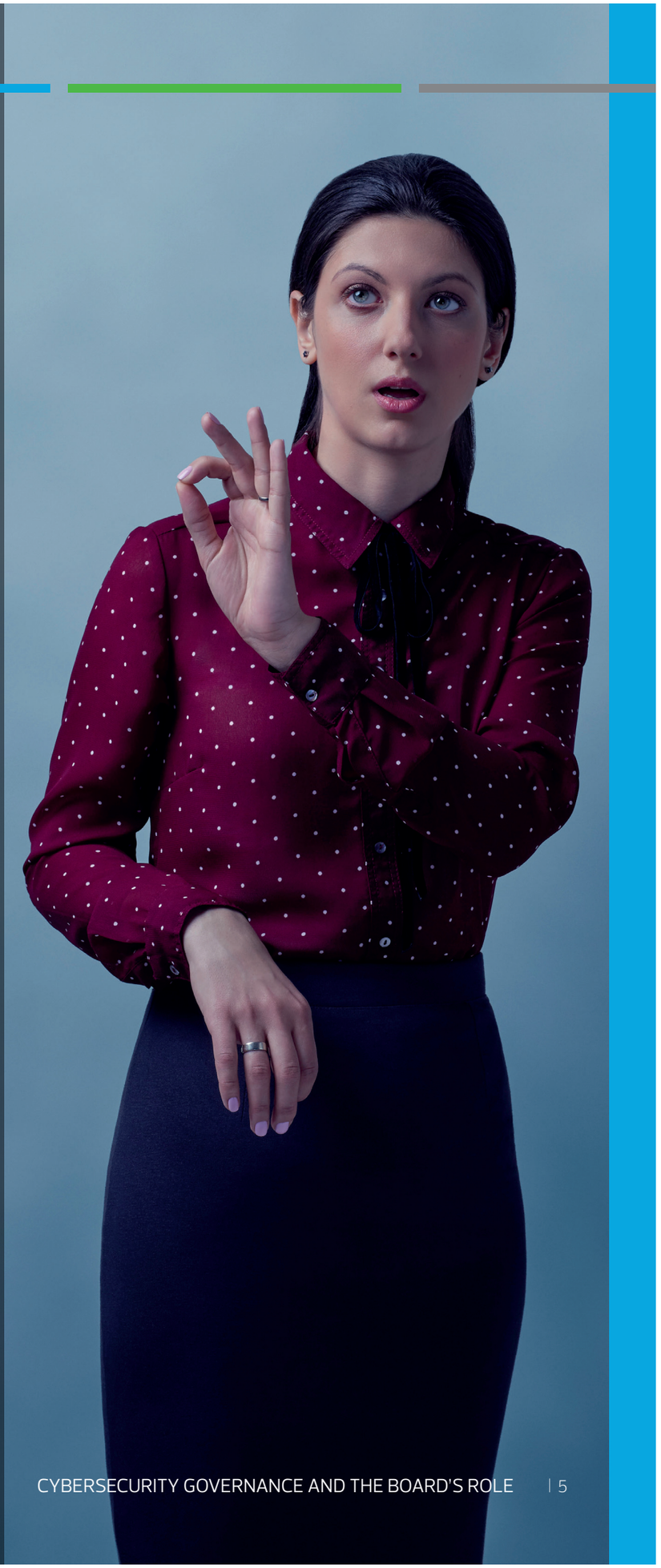
Achieving these objectives will require a substantial commitment from, and possibly a cultural adjustment in, many boards. Companies should also anticipate additional expenditures on internal and external resources needed to address the SEC's proposed requirements if they are enacted. On the upside, board members can anticipate better visibility into cybersecurity risks, and management teams can expect support to address those risks more proactively.

"Regulators and the marketplace are forcing change to close the cybersecurity governance gap. The days of simply attending a board meeting four times a year after reviewing board materials prepared by management are over," said Hackman.

The takeaway

Boards often fail to grasp all the risks that cybersecurity poses to the business—and delegating cybersecurity management solely to the IT department does not work anymore. Without an effective framework in place, many boards may be unprepared for a cyberattack. Your board should proactively evaluate and adjust its processes to ensure full insight into cybersecurity risks and their potential effect on investors.

The good news is, although it is complicated and oversight is challenging, cybersecurity is manageable if your board is open to better understanding it and is willing to dedicate the resources to support it.



Cyber insurance: Is your coverage worth the cost?

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

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

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

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

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

Given the current risk landscape, it's not surprising that most middle market companies have seen rising cyber insurance costs. In this year's survey, two-thirds (67%) of respondents reported increased policy premiums compared with their prior period, with only 2% seeing a decrease.

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

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

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

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

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

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

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

How evolving data privacy regulations **add complexity to operations**

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

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

> "It was very noisy in previous years where privacy was becoming a big debate, but garnering support for overarching privacy legislation at the federal level has been slow-moving in Washington."
>
> **Tauseef Ghazi**
> National leader of security and privacy services, RSM US LLP

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

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

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

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

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

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

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

Among companies familiar with the GDPR,

90% believe it is likely that they will have to comply with privacy legislation in the next two years.

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

Ransomware attacks have declined, but not the perceived risks

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

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

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

In the early days of the COVID-19 pandemic, criminals were quick to strike as many employees transitioned to a work-from-home environment, and data became increasingly decentralized. While companies have done a much better job securing remote environments as time has gone by, potential network intruders are quick to pivot to current issues or seemingly legitimate-looking company information that might strike a chord with users and convince them to click an infected link.

FOREIGN SERVERS

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

SPECIALTY CONTRACTING EXECUTIVE

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

SAVED BY SYSTEM UPGRADES

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

MANUFACTURING EXECUTIVE

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

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

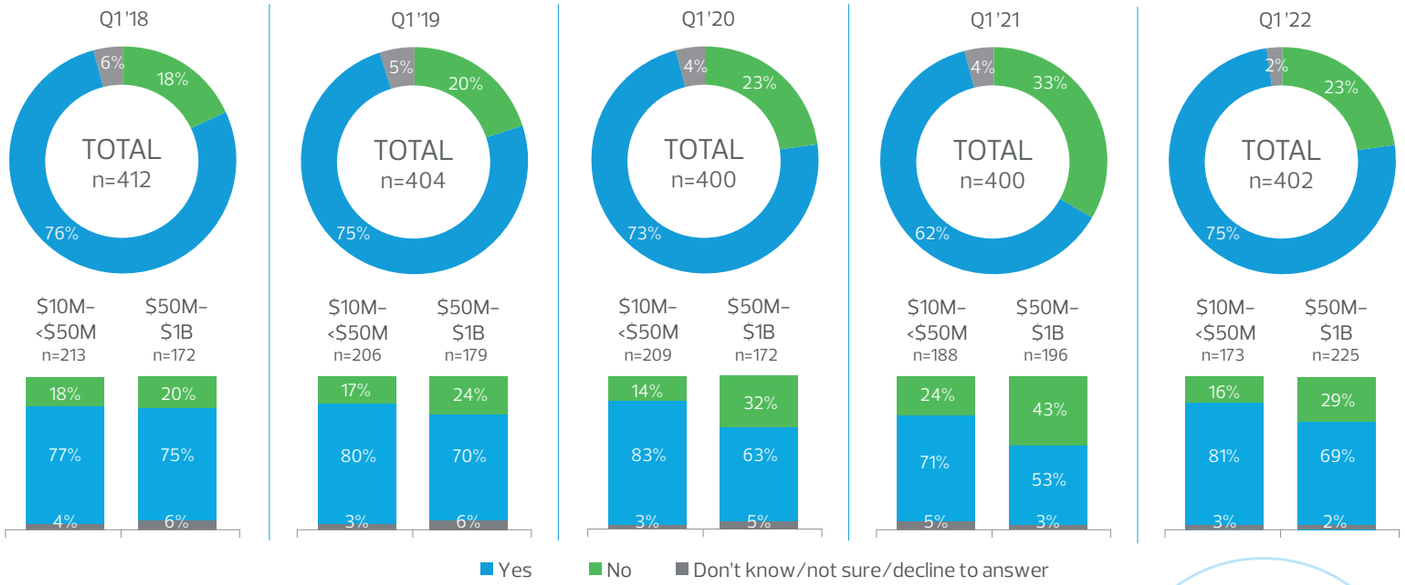
"Companies are implementing multifactor authentication, utilizing more outsourcing and relying on third parties to provide security services," he said. "In the past, there was no endpoint protection and monitoring happening within middle market companies—that was always reserved for larger organizations, given such technologies are not cheap. Now with the introduction of middle market-specific managed security services, costs are reducing, and there is good progress being made, especially in the upper tier of the middle market."

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

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

Experienced a ransomware attack or demand during the last 12 months

(BASE = total sample)



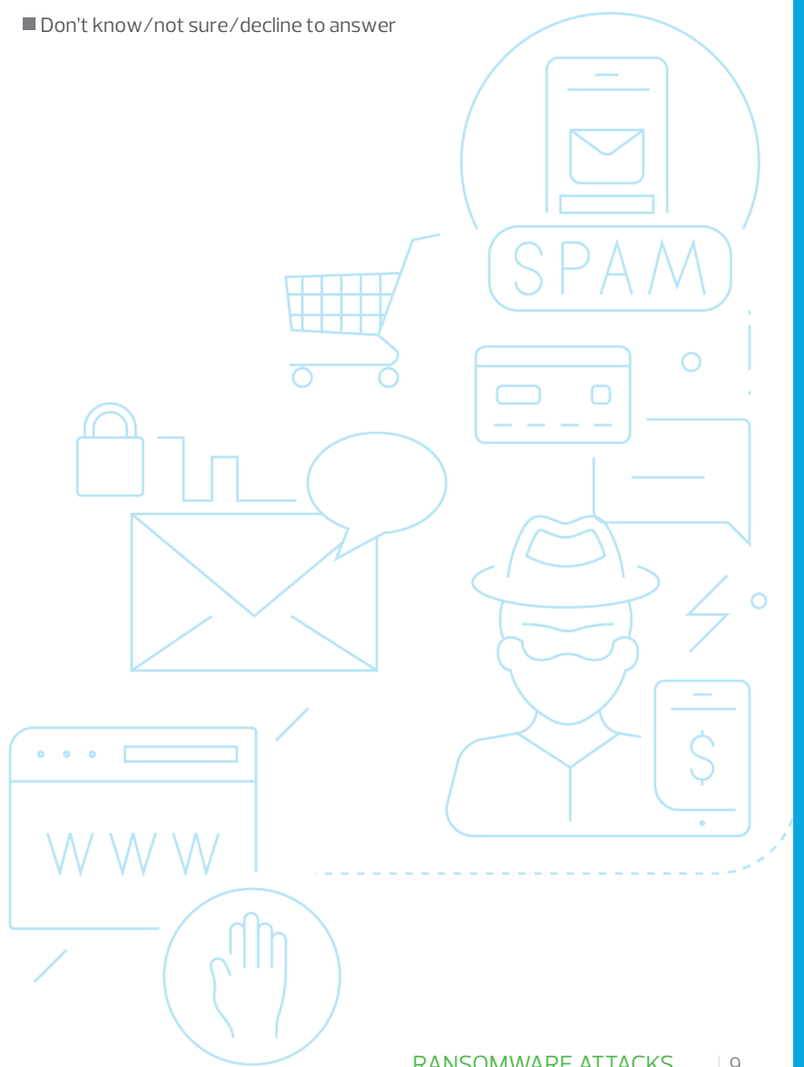
Given their potential for high rewards and relative ease to deploy, ransomware attacks will continue to be a significant threat for quite some time. However, the middle market is certainly making progress and taking effective steps to reduce the frequency and severity of attacks. Companies cannot be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

A FORTUNATE CHANGE IN SYSTEMS

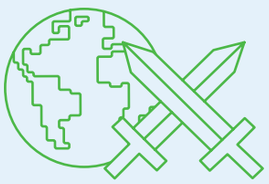
"We recently suffered an attack that originated from Russia. They got into our servers and compromised many files, then required a key. They demanded $200,000 in bitcoin for the key, and the ransom would double to $400,000 in seven days. We did not pay and reported the breach to the FBI, state police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

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

PETROLEUM COMPANY EXECUTIVE



Managing cybersecurity threats related to global conflict



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

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

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

- **Cyber resiliency**—Have an established business continuity plan and maintain an inventory of systems and their established criticality, allowing for decisions to be made by prioritization. Review or develop playbooks for war zone operations, conduct tabletop exercises and test backups for critical assets.
- **Crisis communications**—Establish internal communication procedures, including consistent expectations of regular updates and rapid messaging to employees. External communications should focus on brand protection, engaging with a public relations firm if necessary.
- **System and software updates**—Ensure all systems and software remain up to date, prioritizing updates that address known vulnerabilities.
- **Extended detection and response**—Ensure that endpoint and network protection solutions are installed on all devices, remain up to date and are monitored for unauthorized changes.
- **Increase maturity of identity and access management (IAM)**—Reduce the attack surface by utilizing the principle of least privilege, including the review and removal of unnecessary administrative rights for users and/or shared administrative passwords across devices. Confirm that alerting is configured to detect changes within the IAM system, including privilege escalations and role changes. Utilize multifactor authentication, where possible, on externally accessible systems, such as email, portals and remote access technologies.
- **Security awareness training**—Enhance employee training, confirming that employees are aware of current common threats and how they are delivered. Establish blame-free employee reporting, ensuring that employees know who to contact during an instance of suspicious activity.
- **Review third-party relationships**—Identify critical vendors with operations in affected areas, and ensure that you understand their contingency plans and that they are properly managing their cybersecurity risks. Review contractual language to ensure that it includes appropriate security controls and requirements and document current inventory levels, including on-site and in-transit materials, identifying alternate sources as appropriate. Identify alternate providers as appropriate.
- **Maintain operations**—From a business perspective, review staffing plans for locations affected by the current conflict to maintain critical operational activities. Consider retaining outside legal counsel focused on the continuity of processes.

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

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

"Companies want to take advantage of the productivity, scalability and insight that new innovations offer, but they can't risk leaving themselves vulnerable to a cybersecurity attack in today's risk environment."

—Bill Kracunas, national management consulting leader, RSM US LLP

Understanding cybersecurity risks related to digital transformation

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

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

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

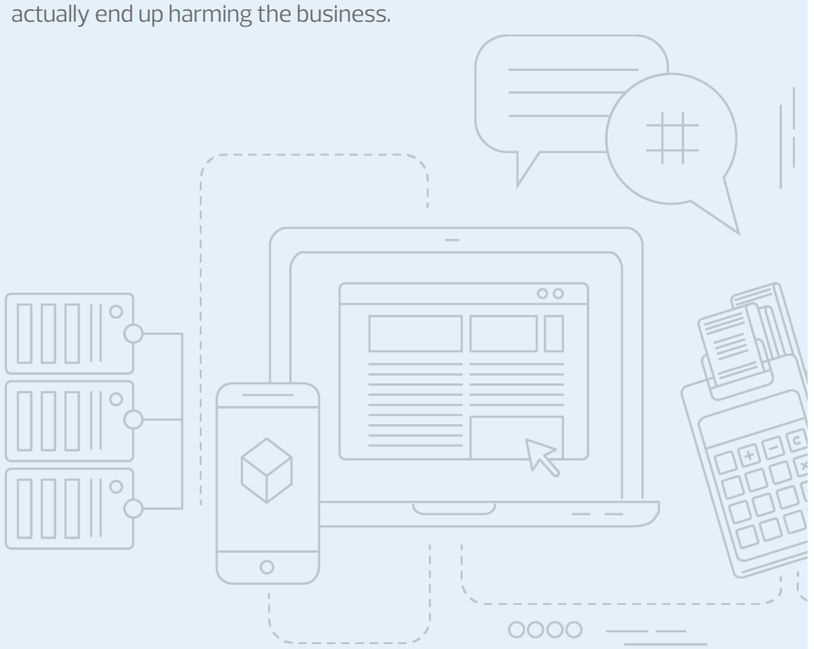
Ken Stasiak detailed how the cloud—and its potential challenges—have evolved. "Moving to the cloud a few years ago was pretty simple," he said. "You had three options. Today, cloud providers offer more options, and it's easy to forget to turn one of these options on or off."

In addition to the cloud, companies are constantly evaluating new customer relationship management and enterprise resource planning solutions, as well as a host of big data and automation applications. And we have yet to scratch the surface of the connectivity and efficiency potential of the Internet of Things. But each of those implementations introduces new access points and new data sources, and organizations need to connect the dots to keep the business safe.

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

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

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



MORE INSIGHTS at rsmus.com

RSM's subject matter experts and thought leaders continually translate what policy developments and macroeconomic trends mean for you and your organization. Visit us now to learn more about these hot topics:

Inflation

Rising costs of goods and services are taking a powerful toll on the economy. Follow the inflation trends and learn what businesses are doing about it: rsmus.com/insights/inflation.html

Industry outlooks

Our industry senior analysts develop data-driven quarterly insights about trends, challenges and opportunities facing organizations in your industry. Learn more: rsmus.com/middle-market/industry-outlook.html

Supply chain

Supply chain snarls persist for many businesses. Learn more about strengthening resiliency and address issues with an enterprise approach. Learn more: https://rsmus.com/insights/supply-chain.html

ESG

Stakeholders' focus on environmental, social and governance issues continues to present business opportunities and important considerations. Stay up to date on the ESG landscape and how organizations are working toward their objectives: rsmus.com/insights/esg.html

For more information please contact
Deborah Cohen, thought leadership and editorial leader
E: deborah.cohen@rsmus.com
or visit **rsmus.com**.

RSM