PROGRESSING THROUGH UNCERTAINTY

How boards can help their organizations stay the course

2023

RSM

Introduction: Uncertainty should not paralyze your business

It would be easy to assert that the last 3 1/2 years have demonstrated how uncertainties challenge businesses. When leaders cannot rely on crucial factors—such as demand, labor, costs, cybersecurity and energy—plans go awry, progress slows and microeconomic disruptions can combine to have macro effects.

The truth, though, is we understood this before the pandemic and its seismic, ongoing economic fallout. Unpredictable disruptions of all types—technology, regulation, policy, war, disease, weather, bad actors, etc.—have always tested businesses' resilience and agility. The difference now is that businesses have more effective resources and tools to insulate against uncertainties and minimize risks.

Automation, data analytics, cyber protections and outsourcing are just a few ways businesses are creating certainty for themselves as the U.S. economy fends off recession.

Those strategies succeeded—into the second half of 2023, at least—despite elevated inflation and interest rates, strained labor markets, tightened financial conditions and softened demand for loans. In mid-July, amid cooling inflation and strong consumer demand, RSM economists downgraded their forecasted probability of a recession in the ensuing 12 months from 75% to 60%, saying it would require an exogenous event, such as a global energy market disruption or a shock via the financial channels.

Of course, there remain challenges that businesses can see and ones they can't. Bloated inventories, hiring difficulties, banking turmoil, technological advances, geopolitical conflicts, swirling political winds—and who knows what else? How businesses deal with those issues and that open-ended question is crucial. In these pages, RSM US LLP offers insights on dealing with uncertainty and minimizing risks so that you can equip your business to thrive no matter what comes your way.

4 steps to funding your ongoing digital transformation

Technology utilization has long been a key differentiator for successful companies. But as new solutions and innovations continue to flood the market, information technology (IT) investments are becoming more difficult to prioritize and manage. Companies may know where they want to invest money, but they might not always know where it will come from, especially in an uncertain economy.

Your company needs to spend on technology for a variety of reasons, from increasing productivity to improving the customer and employee experience and providing more effective security for data and intellectual property. But the decision to make investments and the timing often come down to one critical question: Where are the dollars?

Many companies look at the bottom line and may not see the flexibility for increased technology spending. But there may be a solution to optimize IT investments and discover potential funding. The reality is that not every IT organization is rightsized to meet the needs of the business. However, implementing a four-step process can create an environment that balances spending while uncovering opportunities to implement modern technology resources.

A framework for more IT financial flexibility

Through the following exercises, your organization can gain more visibility into your current IT programs and applications and design a more confident plan for future IT spending.

1. ASSESSMENT

Take a detailed look at your technology infrastructure and budgeting process. How often do you look at those systems? Do you have any visibility into how peers are managing technology and what solutions they have in place? Are you keeping pace with modern technology?

2. TARGETING LOW-HANGING FRUIT

Can any applications or programs be quickly rightsized? Are you paying for more capacity or licenses for certain applications than you need? What quick wins can you take advantage of?

3. EXECUTION

Rationalize your IT framework and investments. Do you have any duplicate systems to combine into one? For example, many companies operate separate customer relationship management systems in different departments. Aligning data under a single umbrella could reduce spending, allowing for additional investments.

4. ONGOING DEMAND AND GOVERNANCE

IT is commonly a reactive department. Ensure you have tight governance in place and encourage business units to make the right technology decisions that align with the digital and technology strategy for the company as a whole. An agile and business-aligned IT department can free up money for ongoing digital transformation while reducing duplication and minimizing off-strategy technology decisions that result in system proliferation, reduced interoperability and increased cost.

When structured right, this framework can be a recurring exercise to evaluate IT resources, identify gaps and discover potential additional funding for adoption of emerging innovations.

With the possibility of a looming recession, value will become more important. Investments in technology cannot stop, but they will likely come under more scrutiny. A periodic look at your strategy can help you identify opportunities behind the technology and create more flexibility through several tactics, including turning off dimensions, adjusting support or addressing individual departments that may have their own digital strategy.

As an additional byproduct of streamlining IT finances, the chief information officer or other technology leaders can become more strategic resources to your entire leadership team, providing guidance on maintaining digital progress in calm economic waters or during potential downturns.

A framework that evaluates the true value you receive from your technology investments amounts to an ongoing transformative exercise that funds itself.

Common risks and opportunities audit committees should consider

An internal audit can do much more than just prepare your organization for an external audit, acquisition or public offering. An intentional approach can yield strategic benefits by providing useful insights, identifying competitive advantages and protecting your company's assets.

But investing resources in your internal audit function can be a tough sell to your board's audit committee. They need to know exactly how this investment will pay off in terms of reducing risk and increasing opportunities.

These key risks and opportunities can help your audit committee see the power and potential of a robust internal audit function.

RISK	OPPORTUNITY
Internal controls One of the most common use cases for an internal audit is ensuring that internal controls are working effectively. This gives you a baseline idea of your company's financial health before you begin an external audit. It will also help you identify areas of improvement that could reduce compliance risk.	**Increased efficiency** Internal audits can help you evaluate the overall effectiveness of systems and processes to identify opportunities for improvement. With regular internal audits, you can tweak processes and make larger adjustments to maximize profitability. This type of oversight can be particularly useful given today's talent shortage, where a lack of expertise and experience with certain functions can lead to errors and inefficiencies.
Fraud Through internal audits, companies can monitor employees for suspicious or risky behavior, which can help to identify and prevent potential missteps or fraud. Performing penetration testing and looking for proper credentialing and system access are also important.	**Competitive advantage** Understanding how your company stacks up against competitors and industry benchmarks can support strategic and tactical decision-making. Internal audits can ensure that your business stays ahead of the curve by providing information about emerging trends and threats. You can use the knowledge gained to avoid unexpected risk and capture new opportunities.
Strategic threats An internal audit function is a critical support system for your enterprise risk management program. Audits can offer visibility into whether you've identified and managed risks related to strategic goals, helping you to stay on track. Regular auditing may also reveal new or emerging risks that were previously unidentified.	**Objective insight** The internal audit function should serve as your organization's trusted advisor. Internal auditors are in a great position to connect the dots within the bigger picture, as well as notice warning signs and gaps that others may have missed. With the right level of independence and objectivity, they can serve as a clear-eyed catalyst for positive change.

Taking the next step with internal audit

Properly developed, an internal audit function offers multiple benefits to an organization beyond simple compliance—regular audits can reduce strategic threats and create opportunities by increasing efficiency and competitive advantage.

Rethinking risk assessments: From checking the box to creating competitive advantage

Conducting a comprehensive risk assessment is just the beginning of digital risk transformation. By using assessment results to reduce risks in a meaningful way, companies are also likely to find new ways to improve operations, enhance information protection, ensure better regulatory compliance, and improve enterprise governance, risk, and compliance (eGRC) capabilities. However, these benefits don't appear magically. Executives must use risk assessments to guide improvements and create a competitive advantage.

1. Recognize the importance of risk assessment to business success

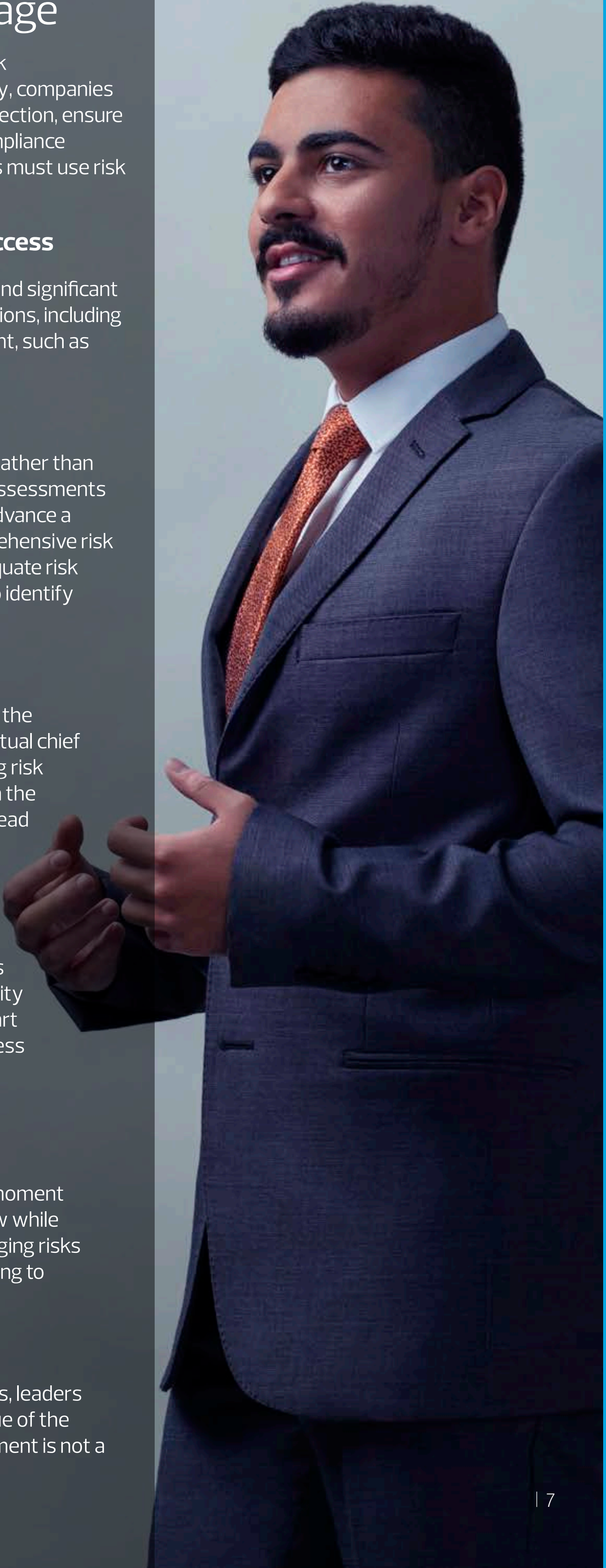
Risk assessments are important tools for identifying and acting on immediate and significant risks. However, they can also generate compelling insights into company operations, including strengths, weaknesses, and potential opportunities for growth and improvement, such as improved internal process efficiency.

2. Make the business case

Your company can use risk assessments to build a business case for changes. Rather than centering on narrowly focused risks at the department level, for example, risk assessments can become the basis for organizational changes and improvements that can advance a range of strategic goals. For example, many private equity firms conduct comprehensive risk assessments on all target companies to make sure those companies have adequate risk and internal controls management in place before closing; those results can also identify opportunities to create value within the organization.

3. Act on what you find

Risk assessments offer a wealth of insights that can identify targeted action at the company, division and department levels. Actions might include establishing virtual chief information security officer and eGRC programs, modernizing and reengineering risk management activity at the department level, and spending more efficiently on the most pressing and strategic areas of risk across the business. For example, instead of layering on new controls, your company could change a business process to reduce risk and improve controls without adding expense and disruption.



4. Support digital transformation

Most large and middle market organizations are making significant investments in digital transformation. Evaluating risks and enhancing risk management activity as part of an interdisciplinary approach to risk transformation is an important part of that process. This can include gauging the relevance of each risk to the business and identifying remediation needs and capabilities in security, data protection, regulatory compliance and other important functions.

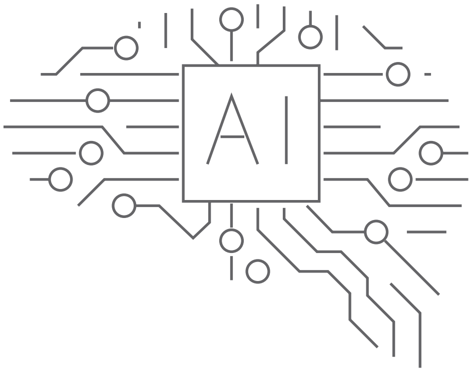
5. Build a lasting risk framework

Risk assessments create a detailed picture of your organization's risks at one moment in time. By building a risk framework, your company can address those risks now while also helping to ensure risk management and controls respond to new and emerging risks over time. Such a framework supports an ongoing and holistic view of risk, leading to appropriate risk mitigation and control activities throughout your organization.

An enduring advantage

To realize the competitive advantage of improved risk management and controls, leaders must go beyond a typical risk assessment, identifying ways to leverage the value of the assessment and its findings. This is the first step to ensuring that a risk assessment is not a one-and-done exercise but a strategic investment in your business.

Rising AI adoption increases the complexity of digital risk governance



Boardrooms continue to face seemingly unending governance, disclosure, regulatory and legal challenges related to digital systems risk. This is exacerbated by the rapid adoption of artificial intelligence (AI), a digital technology that society is just beginning to grapple with and understand.

AI is yet another digital tool that businesses must employ to compete, and it is more powerful than most others. Digital tools have evolved rapidly, their application expanding from segmented IT functions into the central nervous systems controlling the most vital assets and systems in all sectors of the economy, both private and public.

Highly sophisticated AI applications clearly increase potential cyber-risks from external threat actors. In addition, they introduce new, more complicated risks that are perhaps more consequential. Among the many examples are the introduction of biases, unintentional violation of laws and regulations, data exfiltration and erroneous decision making. The growing complexity and persistent nature of AI and cyber-risk are daunting. Boards are on the defense as they deal with new demands for enhanced digital systems oversight.

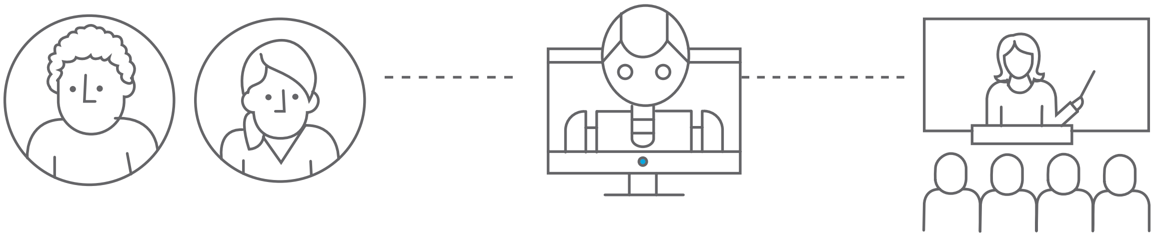
In addition, the technical complexity of risks associated with digital tools is widening governance gaps between the board and risk managers. Digital risk transcends typical business risk. Defensive measures commonly employed by risk resources, such as compliance and risk assessments and enhanced disclosures, are all vitally important but alone do not constitute acceptable governance. The results of these processes are often communicated using technical language that lacks the business context boards need and should demand.

However, despite this deficiency, board members often derive false comfort and accept these measures as meeting their governance obligations. Instead, boards need to develop better context associated with digital risk. This requires understanding the systems being governed and establishing digital risk frameworks, policies and procedures to govern them. Accomplishing this requires organizational, educational and cultural changes to your enterprise.

Organization

Reorganize your enterprise risk and digital systems management and governance structure.

- Ensure your structure fits the size of your enterprise. One size does not fit all. Smaller companies might only engage a chief information security officer (CISO) as a service, while large organizations might employ chief risk officers, chief information officers, CISOs, business information security officers and so on.
- Given the magnitude and growing complexity of digital systems risk, consider establishing a chief systems officer (CSO), or equivalent, position with responsibility and authority over all digital systems. The complexity of digital tools requires careful delegation of responsibilities, authorities and access controls. The CSO must have:
  - Clear authority over information technology, operational technology, legal, internal audit, compliance, finance, human resources, etc., to the extent these functions affect enterprise-wide use of digital systems
  - An independent reporting channel to executive leadership
  - A role as a peer to C-suite executives
- Establish an internal digital risk committee (DRC) led by the CSO to include leaders of all functional areas of the enterprise. This committee will be tasked with managing digital risk and making recommendations to the board of directors.
- Establish a chartered risk committee of the board with a mandate to oversee digital risk. Add digital systems expertise to the board. This committee should interact with the CSO and DRC on periodic and as-needed bases. Be mindful that a separate committee does not relieve the responsibility of the full board for risk oversight.
- Establish enterprise risk management and digital risk frameworks based on DRC recommendations. These frameworks will evolve as digital systems evolve and as the education process within the enterprise matures.



Education

Learn to contextualize digital risk as a systemic risk.

- Digital risk is a form of systemic risk that can only be dealt with through a contextual understanding of the underlying system and subsystems. Without this, the application of risk protection and mitigation methods lacks context and can be both wasteful and suboptimal.

  All private and public enterprises should be defined within a systems context—for example, enterprise as a system (EAS). The EAS is a regularly interacting and interdependent group of elements and subsystems that constitute the operation of the enterprise. EAS elements include assets, processes and the people who interact with one another both internally and externally. Some elements are more valuable than others.
- Develop governance over the EAS through a four-phase process:
  - **Phase 1**: Task the CSO and the DRC to produce a high-level business process map of the EAS for the board, identifying and describing system elements, their importance and how they interact with one other. Describe the digital threat landscape of the EAS. This should be presented using plain English, not technical jargon. Use outside advisors as necessary.
  - **Phase 2**: Conduct a more detailed business process analysis for the CSO, summarized for the board. This analysis breaks down the larger elements identified in Phase 1 into an array of smaller elements, thereby fostering a better understanding of the EAS overall. This leads to a better contextual understanding of the relative importance of your assets and enables better digital risk mitigation investment decisions.
  - **Phase 3**: With the benefit of context established in Phases 1 and 2, conduct a control/framework analysis identifying, assessing and determining the efficacy of digital risk mitigation tools and control activities. Redesign the EAS to reduce the threat landscape and improve control efficiency. Add or consolidate the use of digital risk mitigation tools to produce optimal results. Develop a risk appetite defining the risks the enterprise is prepared to accept in pursuit of value.
  - **Phase 4**: The board and CSO team now have a more complete cyber picture of the digital risk posed to the EAS using language and terms understood by all. It should be reevaluated periodically and episodically when changes are introduced, such as new digital systems, modified business goals, or merger and acquisition events.

Culture

Stress the importance of shared responsibility for controlling digital risk.

- People are the most important component of the EAS. Implementing the organizational and educational steps outlined above will signal the importance of digital risk to the entire enterprise. Elevate the mitigation and control of digital risk from an IT function to a responsibility shared by all constituents.
- Develop an enterprise-wide training program with frequent, short periodic training episodes that do not overburden employees.
- Communicate to all constituents any emerging threats to digital systems and actual incidents experienced by the enterprise.
- Market within your enterprise the importance of controlling digital risk, and reward good behavior.

Establishing a risk foundation

Effective digital risk governance requires boards to demand organizational changes necessary to manage and control complex digital systems, educational changes to develop a common contextual system, understanding among the board and risk management stakeholders, and cultural changes to imprint upon the organization the importance of a shared responsibility for controlling digital risk. The alternative is to remain reactive with unknown consequences, and the stakes are only getting higher as AI capabilities advance.

Embracing 'zero trust': A new era in cybersecurity

As the digital landscape evolves, so too does the threat landscape. The shift toward decentralized networks, cloud computing and increased mobile access has significantly changed how companies need to approach cybersecurity. Today, the traditional perimeter-based security approach is no longer enough to protect systems and data. "Zero trust" is a comprehensive approach to security that operates on the principle of "never trust, always verify."

The essence of zero trust

Zero trust is not a product or a service; it's a philosophy and a strategy supported by people, process and technology. The "never trust, always verify" approach argues against the automatic trust of anything within an organization's network perimeters, insisting that everything trying to connect to a system must be verified before access is granted.

This model emphasizes features such as least-privilege access, micro-segmentation of networks, human and system identity and access management (IAM), and continuous monitoring and security analytics. These components ensure that only the right people have the right access at the right time, and even then, their activities are continuously monitored for any suspicious behavior.

Zero trust and cloud security

As more businesses transition to the cloud, maintaining secure access to resources becomes increasingly critical. In a cloud environment, the traditional network perimeter dissolves, making the zero-trust model's emphasis on verifying every access request, regardless of source, even more relevant.

Cloud security solutions supporting zero trust often provide features such as micro-segmentation, data encryption, intrusion detection and prevention systems, and security configuration management. These tools ensure that your cloud resources are segmented, encrypted, monitored and securely configured, thereby reducing the risk of data breaches.

Identity and access management

A critical component of zero-trust architecture, IAM is employed to identify, authenticate, and authorize individuals or groups to have access to specific applications, systems or networks based on their identities.

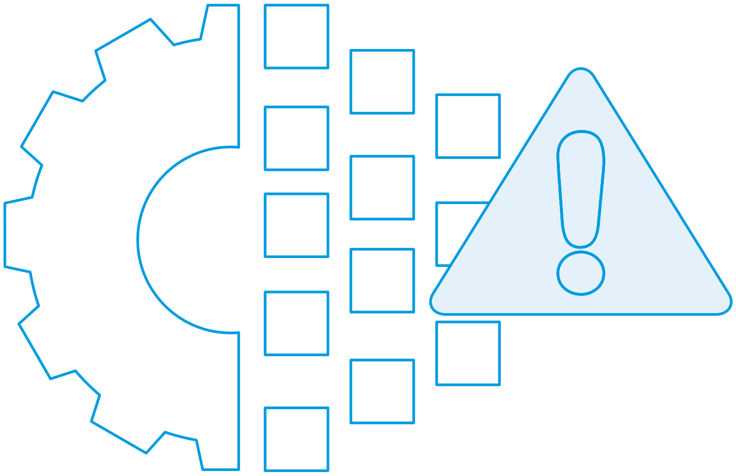
IAM plays a key role in supporting the zero-trust model by implementing multifactor authentication, least-privilege access, identity governance and risk-based authentication. By integrating these features, your organization can add significant protection to your networks and data, ensuring people have access only when and where they need it.

The road to zero trust: Risks and challenges

While the benefits of a zero-trust architecture are substantial, implementing this approach is not without challenges and potential risks. Operational disruption, significant upfront costs, complexity of implementation, compatibility issues with legacy systems, potential impact on user experience, lack of requisite skills and knowledge, and the need for continuous monitoring and adaptation are among the potential obstacles.

However, with the right guidance and support, businesses can manage these challenges effectively. Key steps include:

1. **Minimizing operational disruption** using a phased implementation strategy.
2. **Optimizing costs** by identifying the best-fit solutions that align with your budget and offer the highest return on investment, considering both the upfront costs and the long-term benefits of reduced security incidents.
3. **Reducing complexity** with the help of professionals who can explain your current security posture, design a zero-trust architecture tailored to your needs and assist with its implementation.
4. **Managing legacy systems** and either incorporating them into the zero-trust architecture or pursuing secure alternatives where necessary.
5. **Balancing security and usability** to ensure an effective user experience that enables employees to work efficiently and securely.
6. **Transferring skills and knowledge** from zero-trust professionals to your IT staff, enabling your staff to manage and adapt to the new architecture and the overall security environment.
7. **Continuous monitoring and adaptation** using tools and strategies that account for new threats, ensuring your zero-trust architecture remains effective and up to date.



Cybersecurity: By the numbers

Out of more than 400 middle market leaders surveyed for the 2023 RSM US Middle Market Business Index Cybersecurity Special Report:

20%
Admitted to a data breach in the past year.

68%
Anticipate unauthorized users will attempt to access data or systems in the next year.

63%
Feel that their organization is at risk of a ransomware attack in the next 12 months.

76%
Believe their company is at risk of an attack through employee manipulation in the next 12 months.

Middle market organizations are actively upgrading defenses and implementing new solutions to avoid costly breaches. Their approaches include:

61%
Updating security protocols

61%
Utilizing a cyber insurance policy to protect against internet-based risks

49%
Enhancing the security of existing remote workforce solutions

49%
Strengthening staff training and education efforts

36%
Moving or migrating data to the cloud as a result of security concerns

MORE INSIGHTS at rsmus.com

RSM's industry professionals and thought leaders continually translate what macroeconomic trends and uncertainties mean for you and your business. Visit us now to learn more about these hot topics:

Economic headwinds

The U.S. economy has remained resilient amid elevated inflation and interest rates. Whether that will continue as households spend their excess savings remains to be seen. Stay updated on the latest macroeconomic conditions: https://rsmus.com/insights/economics.html

Digital transformation

Evolving generative AI tools are advancing the digital transformation imperative. Such exciting capabilities come with myriad business considerations. Stay informed about the opportunities and challenges ahead, and look for our special report in late September: https://rsmus.com/services/digital-transformation.html

Critical issues for boards and audit committees

Directors with a 360-degree view of their competitive marketplace can anticipate challenges and lead with confidence. Learn more about how business leaders can help maintain stability as they move forward and seize opportunities: https://rsmus.com/insights/critical-issues-for-boards-and-audit-committees.html

For more information please contact
Deborah Cohen, Thought Leadership and Editorial Leader
E: deborah.cohen@rsmus.com
or visit **rsmus.com**.

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute assurance, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent assurance, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM