PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

2023 Risk Outlook: A Rocky Road Lies Ahead

By Lawrence Baye, CMC, CISA and Mark Bednarz, CPA, CISA, CFE

As we enter 2023, we are facing another year of uncertainty marked by high inflation, the possibility of a recession and the evolving health and safety concerns related to what some call a "triple-demic" with multiple respiratory viruses now in circulation. While last year's supply chain disruption has somewhat improved, unfortunately many small and midsized organizations struggle to attract and retain talent and the cases of fraud and cybersecurity incidents keep rising. When risks occur together or in sequence, organizations are forced to respond to multiple threats or emergencies which can easily spiral out of control and lead to a crisis.

Whether you are serving on a Board, a member of senior management or a business owner, individuals in leadership roles should have a solid understanding of the risks and challenges your organization may face and take steps to reduce the likelihood of occurrence and potential impact. Otherwise, if the event or situation happens, you may experience operational disruptions, financial loss, reputational damage, litigation, or some other undesirable outcome. To help you get started, here are some key risks that have a high likelihood of affecting many industries in 2023.

Uncertain Economic Trajectory

The Federal Reserve is committed to stabilizing prices and gaining control over inflation, which has reached levels last seen in the 1970s–1980s. Whether inflation is the result of ongoing geopolitical conflicts, trade wars, changes in demand, supply chain issues or various other factors, some organizations have started to defer spending and delay (or shrink the size and scale) of capital projects and certain large public companies have announced headcount reductions after adding staff over the past two years to keep pace with consumer demand. In the last year, consumers have altered their buying habits to save money by prioritizing food, fuel and other basics over less essential items and turned to discount stores and e-commerce sites offering lower prices and private label products.

Since few of today's leaders were in senior positions four decades ago, absent a playbook to rely on, you may want to start by asking the following questions:

- Are we forecasting our financial performance over the next few years under different scenarios and determining what actions would be required in terms of headcount, spending and other commitments? Will we be able to support our operations, programs and initiatives at current levels?
- Are we closely monitoring our cash burn rate and capable of predicting the timing of anticipated receipts and disbursements? Can we paydown expensive debt and/or tap existing lines of credit for emergencies?
- Can we accelerate the collection of billed receivables, use incentives to spur customer payment and offer discounts to drive incremental sales, especially if we have idle capacity or excess/slow-moving inventory that can be converted to cash to avoid carrying them into a future season?
- Do we have the option of delaying vendor payments and having them provide us with extended terms?
- Can we cut our occupancy costs by shrinking our footprint, using hoteling, evaluating flexible work arrangements, consolidating locations and subletting space if our leases do not allow early termination?

- Have we assessed our business processes to eliminate inefficiencies, optimized the use of our systems and strengthened the control environment?

- Is our workforce able to handle the planned workload so we can avoid overtime and seasonal labor costs?

Workforce Instability and Employee Health Concerns

Many organizations are still suffering from employee turnover and have difficulty finding suitable replacements; this situation is most acute when a long-tenured manager with institutional knowledge gives notice, there is no trained successor in place and written policies and procedures are dated, incomplete or absent. Unlike larger corporations that tend to have deeper benches, small and midsize organizations typically operate lean, so each loss is challenging because of the impact on day-to-day operations.

One often overlooked issue that contributes to personnel turnover is the continuing cycle of emergencies that employees experience at home or at work. Since the pandemic began, we have seen increases in crime, flooding, high winds and wildfires, ransomware attacks and skyrocketing operating costs of running a household or organization. Vacancies create additional work, a burden borne by the remaining employees. These stressors breed frustration, anxiety and anger and take a toll on mental health and can lead to employee burnout, substance abuse and, ultimately, quitting.

To begin to address these issues, you should know:

- What can be learned from turnover data when analyzed by level, job and location? Do exit interviews shed light on the cause and are the departures indicative of a systemic problem that can be fixed?

- Why have new hires not worked out, have our expectations been realistic and are we providing them with the proper orientation, tools, training and mentoring to enable them to be successful?

- How often do we take inventory of our staff and their skills, compare the results against our present and future needs and then layout a plan to close the gaps? If employees want or expect to further develop their capabilities to take on new responsibilities, how are we satisfying their desires?

- Do we periodically retain compensation consultants to study our salary and benefit structure across job families and locations, assess how our compensation compares to competitors and similarly sized organizations in our industry and geography? If we cannot afford to be on par with others, what else can we do to differentiate what we have to offer to attract and retain talent?

- What programs are in place to promote physical and mental well-being, such as requiring all employees to take time off at different times of the year (and not just bank them), encouraging exercise by subsidizing gym memberships or providing in-office yoga sessions, distributing only nutritional snacks? What about closing early during slow seasons and before holiday breaks, supporting community involvement and volunteering, promoting diversity, equity and inclusion in hiring practices and selecting candidates for advancement and publicizing the availability of mental health professionals as part of medical insurance coverage?

- Do we provide our staff with opportunities to work part-time on a compressed schedule or under a hybrid arrangement, so the jobs are attractive to a larger pool of candidates?

Threats to Reputation, Culture and Compliance

It takes years – and sometimes decades – for an organization to establish its brand name and identity and build a positive image, but a reputation can be destroyed by just one event. All it takes is an embezzlement, corruption, harassment, the sale of defective products or visible service failures to erode the confidence and trust others have in the organization. Even if there is no outside investigation or media coverage of the incident, employees often learn what has transpired and begin to question whether this is the right environment in which to work. In 2022, we have read about government officials, executives, celebrities, sports figures and broadcasters who have been fined, lost their position or were incarcerated due to recent or past affairs, abuse of funds or authority, propagating derogatory, questionable or false statements and using illegal substances.

From an external perspective, it is important for leaders to be fully aware of the information that appears on their websites, annual reports and marketing materials as well as the messages conveyed in press releases, articles, speeches and other public remarks. In addition, they should receive a synopsis of both positive and negative feedback and its source (e.g., customer service complaints, social media posts) and decide whether a response is required to false statements or allegations. It may also be wise to check available information about competitors because often the issues they face apply to other organizations in the same sector so this intelligence can serve as an early warning.

An organization's reputation can be damaged by a toxic culture that hurts morale, lowers productivity and increases the rate of turnover. Effective leaders should create and sustain a positive and healthy workplace that inspires people to trust one another and work together (instead of in silos) to achieve common organizational objectives. Interviews, surveys and focus groups are techniques commonly used to assess whether employees embrace the organization's values and vision, believe that those in leadership positions model ethical behavior, communicate effectively, treat everyone with respect, welcome new ideas and differences of opinion, treat errors as learning experiences as well as recognize and reward individual contributions. Since successful organizations capitalize on opportunities and adapt as conditions change, whistleblower reports, exit interviews and other information may provide valuable insight.

Reputation can also be impacted by compliance failures. Not only are new laws and regulations routinely introduced but existing ones may change. For example, in 2023, there is significant likelihood that new rules will be issued regarding data privacy, disclosure of salary ranges when vacant positions are posted, sanction adjustments on federal watch lists if foreign conflicts subside, health and safety protocols, licensing and permit requirements, etc. As a leader:

- Do you know which laws and regulations apply to your organization and, as new ones are added or existing ones change, how is this information communicated to others and are there different requirements by location to consider?

- Is there an executive or manager responsible for each compliance requirement and who verifies that all compliance and reporting obligations are met and there is evidence retained to support this conclusion?

- If your organization is subject to multiple regulations and overlapping controls, are you leveraging the testing of these controls, so they satisfy multiple regulations and do you retain the control set along with test evidence in a GRC (governance, risk and compliance) repository?

- Do you have in place the three lines of defense; namely, operations, compliance/legal and internal audit? Are they effective?

Rising Fraud, Cybersecurity and Data Privacy Exposures

The Association of Certified Fraud Examiners estimates that occupational fraud costs business trillions of dollars globally and from our own observations, consumers continue to be victimized by identity theft, phishing and account takeovers. Just recently, the press reported that a significant percentage of the federal payments made during the pandemic may have been issued to ineligible recipients and some of these funds were diverted offshore. On the cybersecurity front, bad actors have targeted hospitals, government agencies, public utilities, educational institutions and commercial businesses. No organization is insulated from these attacks, whether their objective is financial gain, the theft of data or to be disruptive.

The pandemic has altered the way most organizations operate, who they do business with and how they leverage technology by enabling online purchasing, utilizing electronic documents with digital signatures, automating workflow and approvals, providing portals for the exchange of information and processing of transactions as self-service functions and deploying collaboration tools to connect the workforce with customers, suppliers, funders, grantees and others they interact with. At the same time, criminals have evolved more sophisticated technology-based schemes by creating phony entities and user credentials for money transfer, using malicious software to collect the information needed to access and control individual or business accounts and placing legitimate-looking online ads that are linked to websites that request payment but fail to deliver the items purchased.

To safeguard against these risks, you should evaluate:

- Whether your policies and procedures, as well as security practices, are robust and have been updated to reflect any operational and system changes made during the pandemic?

- How extensively you vet your customers and vendors before doing business with them? Many organizations have replaced on-premise applications with cloud-based systems in recent years but did anybody take the time to get to know their control environment, fiscal health and incident response and disaster recovery capabilities? Did you review the User Considerations Section of the service organization's SOC 1 or SOC 2 report to ensure you have appropriate internal controls from end-to-end?

- Are your financial controls over the processing of receipts, disbursements (e.g., ACH, credit cards, checks), payroll and other transactions adequate, including treasury or banking activities (e.g., wire transfer transaction authorization)?

- How effective are your cybersecurity practices that cover the technology infrastructure (e.g., networks, equipment, endpoint security, backup and recovery, application and system-software configurations, user access right assignments based on job function/need to know), governance and employee awareness of new threats and schemes and how often are vulnerability scans and penetration tests performed? Do employees and contractors undergo annual cybersecurity awareness training to understand different schemes hackers and other perpetrators use to gain access to the network, sensitive information and funds.

- Do you have protocols in place for data classification based on ownership and sensitivity level? Do you enforce policies over data collection, encryption, storage, management, use, sharing, transfer, retention and naming conventions?

Weather Extremes That Impact Operational Resiliency

While there are ongoing debates about the causes of global warming, climate change has altered weather patterns and the severity and frequency of storms. According to statistics compiled by the National Center for Environmental Information, in 2022, the United States has experienced over 15 major events including hurricanes, tornados, hailstorms, heat waves, droughts, floods and wildfires. While it is commendable that government has taken measures to limit flooding from storm surge, there is uncertainty whether the preparation is sufficient given the strength of these storms and revisions to FEMA maps that show that more areas are subject to flood risk.

As part of business continuity and resiliency planning, every organization should determine how climate/weather changes might affect them by engaging specialists to conduct a resiliency assessment to identify vulnerability points and consulting with government experts who study weather patterns and their damage potential. A specialist might collect information about where the employees live and what alternatives are available for commuting to work if a storm makes roads impassable for driving or shuts down public transportation and make inquiries of the landlord to find out whether basement flooding would make elevators inoperable and pose a hazard to anybody entering a building without lights, power and phones. Further, if the roof collapsed due to the weight of snow or high winds, what office or facility equipment, supplies and records would probably be destroyed?

Digital Transformation Challenges

While most organizations have digital transformation projects either underway or planned, it is likely that you might also be interested in investigating or adopting new or novel technologies to gain a competitive edge, streamline workflow, enhance customer, client or member engagement and improve productivity. Some of these emerging technologies include drones that can be used to inspect infrastructure that is hard to access or deliver products to remote locations, virtual reality for job training, artificial intelligence to analyze patient symptoms for diagnosis and treatment, Internet of Things where embedded sensors detect equipment or vehicle malfunctions and generate work orders to initiate repair and robotic process automation where software handles repetitive tasks formerly performed by humans. These innovations are in addition to expected improvements in network and computer reliability and performance, GPS tracking as a standard option in motor vehicles and other advances in application features and analytical capabilities.

Since most executives do not have formal technology backgrounds or came up through the ranks of the information technology function, you might look to Board members or outside advisors with this knowledge to help evaluate major proposals made by vendors or internal information technology managers. You should advise them that proposals must contain a "business use case" that defines the business problem to be solved, how the project relates to the organization's strategic priorities, what other alternatives were considered, the components of the solution framework, the requested financial support, schedule, resource requirements and milestones/deliverables by phase/stage, potential risks and how they will be addressed, the target return on investment, the research or competitive intelligence that supports the recommendation and the evidence (such as a prototype) that demonstrates that the technology is viable.

As a reminder, some personnel will naturally gravitate toward new technology and even early adoption because they see the benefits, especially if it eliminates routine tasks and allows them to focus on more value-added activities. Others, however, may be hesitant to embrace new systems and might fear that technology will make their jobs obsolete. Management must have a frank conversation as to these changes and impact on their staff on an individual basis to avoid creating additional stressors.

Contact Us

We have assisted clients in conducting risk assessments in the commercial, governmental and not-for-profit sectors and also provided independent reviews of Enterprise Risk Management programs already in place. If you would like to discuss your situation and needs, please reach out to:

Mark Bednarz, CPA, CISA, CFE
Partner
mbendarz@pkfod.com

Lawrence Baye, CMC, CISA
Principal
lbaye@pkfod.com