DATAMINR PULSE

Global Risks and Business Resilience in 2023

Three-plus years since the onset of the COVID-19 pandemic, much of the world has reopened for travel without restrictions. But while it feels like the pandemic—which significantly affected our society in all aspects—is mostly behind us, the global economy now faces new challenges in 2023—starting with a wave of mass layoffs at many of the largest companies in the world.

In addition, global economic growth is projected to sharply decelerate from 3 percent in 2022 to 1.7 percent in 2023—its third weakest pace in nearly three decades—overshadowed only by the 2009 and 2020 recessions, according to the World Bank's most recent economic report. Ongoing geopolitical and fiscal tensions such as the Ukraine-Russia war, higher-than-expected inflation and tough anti-inflationary measures are some of the adverse conditions contributing to this fragile economy.

The World Bank forecasts global economic growth to sharply decline from 3 percent in 2022 to 1.7 percent in 2023. This is the third weakest pace of growth in nearly three decades.

As a result, it's a business imperative that organizations have adaptable and innovative risk management and resilience strategies to better navigate the ever-evolving risk landscape.

Here, we'll explore steps you can take to improve business continuity in today's environment, and better prepare for risks on the horizon.

Build Risk Resilience

Risk-resilient organizations are those that understand the macro factors in which they operate, and build plans that allow them to adapt to changing circumstances, survive sudden shocks and regain a desired equilibrium. Given that the volatility of the business economy will continue in 2023, companies should ensure every facet of their enterprise is built for resilience.

In its 2023 edition of The Global Risks Report, the World Economic Forum (WEF) calls for a rigorous approach to foresight and preparedness to boost resilience to longer-term risks. The report outlines four key principles businesses should follow:

1. **Improve risk identification and foresight.** Identify future developments, risks and opportunities. Adopt tools that provide early warning for when specific risks are about to materialize to enable advanced preparedness measures.
2. **Rethink 'future' risks.** De-anchor risk prioritization from shorter-term incentives and adopt a dual vision that more effectively balances current crisis management with a longer-term lens.
3. **Invest in multi-domain, cross-sector risk preparedness.** As global risks become more intertwined, preparedness needs to become a shared responsibility between sectors, with local and national governments, business and society each playing to their strengths.
4. **Connect resilience efforts with other goals.** For example, shortening supply chains can advance net zero strategies and reduce exposure to adverse geoeconomic developments. Efforts to foster strong community relations can also help recovery initiatives in the event of a disaster.
5. **Rebuild and strengthen global risk preparedness and response cooperation.** Greater collaboration across industries and between countries is critical to help identify signals of emerging threats at both a national and global level.

Organizations must also develop flexible and efficient resiliency models to sustain and streamline operations during crises. These models must be flexible enough to withstand unforeseen disruptions and events as they arise and unfold.

The four must-haves of any resilient organization:

1. A proactive approach to risk management
2. A security-first culture
3. Playbooks and continuity plans
4. Cutting-edge technology

As business leaders look ahead, they can lead the charge in helping to improve business resilience, ensuring their organization can thrive amid disruption and uncertainty. To do so, they should consider adopting the following four crisis leadership behaviors:

1. Understand the risk landscape
2. Adapt playbooks in real time
3. Embrace organizational change
4. Practice making tough, strategic decisions under stress

Identify Threat Vectors

Although the risk landscape is ever-evolving and complex, two threats have remained in the top 10 risks for businesses within the past few years: extreme weather events and cyber crime. According to the WEF Global Risks Report, these two risks are among the biggest concerns of organizations worldwide as they look at the next two to 10 years.

While the COVID-19 pandemic is no longer considered a top threat, supply chain disruptions—a major challenge in 2022—are expected to persist in 2023 and beyond due to cyber attacks, energy shortages and severe weather, according to the Business Continuity Institute's 2023 Supply Chain Resilience Report. As such, organizations need to constantly assess and determine their threat vectors to best prepare for both familiar and unforeseen risks.

It's also crucial to zoom out and view risk management holistically:

- Does your organization have the resources to weather multiple quarters of losses caused by these types of threats?
- Do you have the right security teams and frameworks to protect a dispersed workforce, which is a result of the move to remote and hybrid work models?
- Can your organization shift its distribution model or identify alternate suppliers in case of disruption?

And, as the World Bank has predicted a global recession in 2023, it's even more critical that businesses equip themselves with best practices that can help them survive a potential economic downturn.

Risk and Threat Assesment: 2023 Forecast

2 years		10 years	
1	Cost-of-living crisis	1	Failure to mitigate climate change
2	Natural disasters and extreme weather	2	Failure of climate-change adaptation
3	Geoeconomic confrontation	3	Natural disasters and extreme weather events
4	Failure to mitigate climate change	4	Biodiversity loss and ecosystem collapse
5	Erosion of social cohesion and societal polarization	5	Large-scale involuntary migration
6	Large-scale environmental damage incidents	6	Natural resource crises
7	Failure of climate change adaptation	7	Erosion of social cohesion and societal polarization
8	Widespread cybercrime and cyber insecurity	8	Widespread cybercrime and cyber insecurity
9	Natural resource crises	9	Geoeconomic confrontation
10	Large-scale involuntary migration	10	Large-scale environmental damage incidents

Risk Categories 🟦 Economic 🟩 Environmental 🟧 Geopolitical ■ Societal 🟦 Technological

Source
World Economic Forum Global Risks
Perception Survey 2022-2023.

Manage Crises

All organizations should understand that crises are inevitable. If they haven't already faced a major crisis, it's a matter of when—not if. A well-managed crisis response will lean on the structural work completed earlier, scenario planning and clearly defined roles and responsibilities to contain the impact of the risk event and maintain business continuity.

It's not enough to plan for only one or two years ahead. Organizations must closely study the risks they will likely face, as well as examine how they can strengthen and maintain business resilience and agility with a five to 10-year plan.

Learn More:
The 10 Golden Rules of Crisis Response

Start by identifying previous risk events to understand how and why they happened, and whether your organization is still susceptible to them.

If the risk is preventable, invest in proactive measures to minimize the risk now. This can include improving cybersecurity or ensuring disaster backup and recovery during a network outage.

Build scenario plans for the most common risks you face. Run regular crisis simulations and table top exercises, with an eye toward testing your ability to manage multiple risk scenarios at once. For example, simulate an IT outage during an extreme weather event.

Ensure your planning considers worst-case scenarios. Failure to do so can lead to scenario plans with hidden gaps.

A Real-world Cautionary Tale

Prior to the 1993 World Trade Center attack, Morgan Stanley head of security Rick Rescorla repeatedly warned of potential terrorist attacks and requested additional security—and had identified a significant vulnerability in the building's garage, where the attack took place. Although his warnings were not heeded, his continued surprise evacuation drills and scenario planning are credited with saving the lives of more than 2,600 Morgan Stanley employees during the September 11, 2001 World Trade Center attack.

During a crisis, your organization's response is only as good as the information it uses to make decisions.

Outdated or inaccurate information can hinder your ability to act—and even widen the impact of a crisis. Organizations that want to reduce the impact of a crisis need fast, accurate and relevant data

For example, organizations that rely on Dataminr's real-time alerting solution, Dataminr Pulse, receive the earliest possible indications of emerging risks and high-impact events, giving them more time to assess and direct the right resources quickly and efficiently.

Take for instance a U.S. healthcare system with approximately 30,000 employees and more than 100 hospitals and clinics. Since using Pulse, the healthcare system has been able to more effectively identify and maintain updates on all major security concerns for its locations, as well as ensure the duty of care for the employees and patients at each of those facilities.

German financial institution Deutsche Börse relies on Pulse's real-time information to detect emerging risks and events and has been able to significantly reduce its crisis response time as it's often informed of incidents within seconds or minutes of an occurrence.

Improve Risk Management to Maintain Business Continuity

In the aftermath of a crisis, it is imperative for companies to have an understanding of their exposure, vulnerabilities and potential losses to prevent future disruptions and ensure business continuity. Consider the potential money lost, brand and reputational damage, as well as effects on employee morale, third-party partners and suppliers.

- Identify where and when your risk management plans worked and failed, or at least merit improvement. For example, how long did it take for your team to issue its first public statement about the crisis, relative to public awareness of the original incident that triggered the crisis? Could that time frame have been accelerated?
- Determine what information was missing, as well as the data points you were aware of, but didn't act on early enough.
- Document your learnings so that your security team and key partners can improve future responses.

It's difficult to predict when an incident will next occur, and what the type, scale and scope will be. As such, it's in every business' best interest to ensure they have a comprehensive and effective enterprise risk management (ERM) program that helps them better navigate risk and strengthen business resilience.

Whether you're building or optimizing an ERM strategy, consider the following best practices to ensure you're on the right path to success:

- Audit your risk management strategies
- Remove silos, increase coordination and lay the groundwork for automation
- Improve strategy and consolidate technology investments
- Drive ongoing optimization and demonstrate how your business is prepared to respond to evolving risk

In an ideal world, we'd never encounter unexpected disruptions or crises. In reality, they occur with a higher frequency than people care to admit. Planning for them as best as possible and implementing real-time alerting solutions ensure your organization can effectively respond to disruptions, mitigate their impact and quickly recover.

Learn More:
3 Mistakes to Avoid When Implementing an Enterprise Risk Management Program

Learn More

Find out how and why organizations like yours rely on **Dataminr Pulse** to maintain business continuity and strengthen their resilience.

DATAMINR PULSE