Healix

Risk Radar 2024

Dare to Prepare

November 2023

Welcome to our all-new Healix annual report, Risk Radar 2024: Dare to Prepare

This year, we're taking a different approach to our outlook on risk by talking to those on the frontline of risk management for their organisations.

We commissioned an external research team to speak to risk managers, senior security managers and travel risk managers at mid-sized businesses across multiple industries. We asked pertinent questions around their current risk strategies and practices, to understand where they perceive their priorities and challenges to lie. In total, we received 500 responses across Construction, Energy & Mining, Financial and Professional Services, Higher Education, Technology, Manufacturing, Media and Entertainment and Not-for-Profit.

We collated responses across 20 questions and this report features key findings from the data, pulling out three themes that we believe to be the most revealing. We also share insight into these risk factors to underpin strategic decision making, while also taking a deep dive into regional pictures for the next twelve months.

Director's view -

Chris Job, Director of Risk Management Services

In the world of risk management, the only constant is change and I am reminded of the familiar phrase "no plan survives first contact with the enemy". This maxim is apt in the face of recent global events.

The assault by Hamas from the Gaza Strip into Israel in October 2023, marked by a barrage of attacks and hostage-taking, took us all by surprise. Healix swiftly activated its Incident Management Team (IMT) to assist those clients seeking our help, from advice to evacuation.

Fresh in the memory is the Wagner Group plane crash in August that same year. The loss of three senior influential leaders, including head of the organisation, Yevgeny Prigozhin, along with three other key figures crucial to operations, highlights a critical concern within risk management – the concentration of key personnel in a single, vulnerable situation. This incident illustrates that no organisation, no matter how experienced or assured, is immune to risk.

These global events, whether directly affecting us or not, serve as a salient reminder to revisit our own plans and procedures. Are they still fit for purpose? When was the last time we stress-tested them? Do we have relevant and appropriate risk mitigations in place? The importance of preparing for the unexpected cannot be overstated. Healix's IMT, tried and tested through numerous activations, stands as testament to that. Recent responses to Afghanistan, Ukraine, Sudan and now Israel underscores the fact that complacency is not a risk management strategy, and we work hard to ensure that we are properly prepared and ready for whatever happens.

A year ago, we highlighted the surprisingly low awareness of the best practice guidance, ISO 31030. Now two years since its publication, with business travel continuing to rise, our recent survey has highlighted a significant increase, with 76% of respondents reporting they have now reviewed their travel and people risk management programme in line with ISO 31030.

Of equal importance is the recognition of the role of personal risk profile, on par with more traditional risk factors like security risk environment, availability and quality of medical care, and nature of activities. Our survey reveals that grappling with personalised risk remains a challenge, despite many respondents acknowledging its critical role in the incidents that they have managed. This is already something we're responding to – evolving our recently launched Healix Travel Safe to encompass other personal risk factors and associated risk mitigation measures.

I hope you find the report insightful and that it gives pause for thought on the priorities for risk management planning in 2024.

1. The rising tides of risk

Managing the traveller

80%

of our survey respondents said that they have managed an incident relating to traveller's personal risk profile

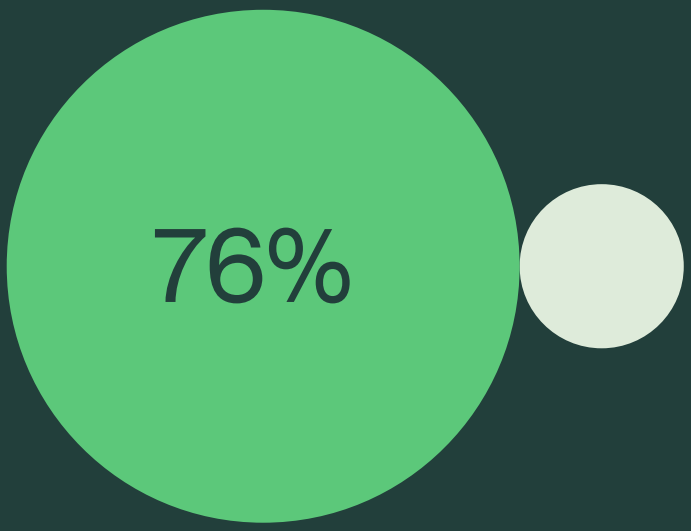
39%

of the same people look at personal profile as part of travel risk assessments

Gender identity and sexual orientation was ranked the

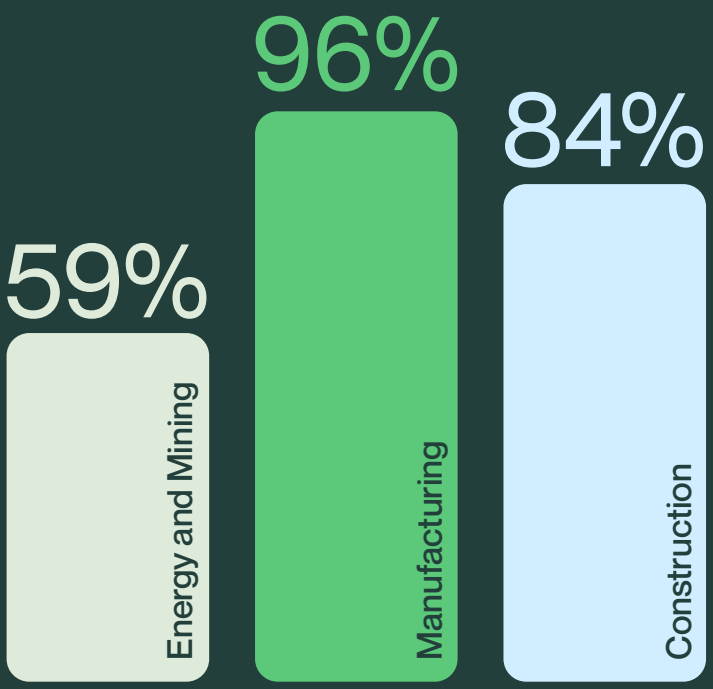
No.1

factor impacting a traveller's personal risk profile in the Higher Education sector



76%

of our research respondents said that they had reviewed their travel risk management programme in line with ISO 31030



Breakdown of adoption of ISO 31030 across sectors

Now it's personal

At a recent roundtable event, we had the privilege of hosting speakers from PwC and the BBC to delve into the realm of personalised travel risk. Among the attendees were prominent business leaders from industry giants such as Apple, Credit Suisse, Deutsche Bank, and Meta.

This high-powered assembly serves as a testament to the growing recognition of the significance of personalised risk assessment within our increasingly complex operating landscape.

Personalising the risk assessment process adds an extra layer of protection, departing from the outdated 'one-size-fits-all' approach. It embraces nuance and recognises the distinctive circumstances and characteristics of each traveller. Factors like demographic profiles, mental and physical health, and travel experience play a pivotal role in shaping individual risk exposure and perceived safety levels. In essence, this approach enables an organisation to tailor its risk management strategies to suit each traveller, enhancing their effectiveness in mitigating and managing travel-related risks.

As part of our research, we sought to gauge how businesses incorporate personal risk profiles into their risk assessments. Interestingly, 80% of our survey respondents reported having managed incidents linked to a traveller's personal risk profile. However, only 39% of these same individuals integrated personal profiles into their travel risk assessments. Why this discrepancy?

Our roundtable discussions highlighted a common challenge: collecting and using sensitive data without breaching trust. Employees may be hesitant to share personal information, making it vital to demonstrate the benefits of opting in. In essence, the more information shared, the safer and better informed travellers can be. This isn't just about data security; it's a shared effort to enhance safety and improve the overall travel experience.

Travel with pride

Gender identity and sexual orientation are increasingly becoming key factors in personal risk profiles. Many countries still criminalise individuals based on these preferences, warranting careful consideration for travellers visiting such regions.

Our research uncovered that in the Higher Education sector, gender identity and sexual orientation rank as the primary factors impacting a traveller's personal risk profile. This industry is commonly associated with being an advocate for progressive change and ally-ship, and a safe place for students to openly express their identity. They also host a significant number of Generation Z students, where one-in-five Gen Z adults identify as LGBTQ+ and an expectation for these numbers to continue to rise each year.

Legislative changes worldwide continually impact LGBTQ+ travellers, who face a multitude of legal, social, and cultural risks when journeying across the globe. For instance, Canada recently updated its travel advisory, warning its LGBTQ+ citizens about the potential impact of US laws on their travels. Examples like this underscore the nuanced nature of personal risk profiles, emphasising the importance of understanding the legal and cultural landscapes employees may encounter to mitigate risks effectively.

Setting a standard

The prominence of personal risk takes centre stage within the ISO 31030 guidance, a pivotal framework that emphasises that effective travel risk management extends beyond having an understanding of environmental risk factors alone.

Introduced two years ago, ISO 31030 serves as benchmark for businesses, applying to a broad spectrum of organisations and various risk scenarios. But how seriously are businesses taking it?

A notable shift in awareness is evidenced in our research, with a noteworthy 76% of respondents indicating that they have reviewed their travel risk management programmes in alignment with ISO 31030.

‘The future of ISO 31030 holds promise’

Back in April last year, a survey by Business Travel Show Europe highlighted that most travel buyers remained unaware of ISO 31030, so our results suggest it is gaining momentum. The Global Business Travel Association (GBTA), for instance, now features a request for proposal (RFP) template with a central focus on ISO 31030, underscoring its increasing relevance to business.

Our research further reveals that the varied adoption of ISO 31030 across sectors can be attributed to timing. For instance, while Energy and Mining sectors show a review rate of only 59%, Manufacturing and Construction sectors are leading with impressive percentages of 96% and 84%, respectively. The divergence in adoption timelines reflects unique industry dynamics.

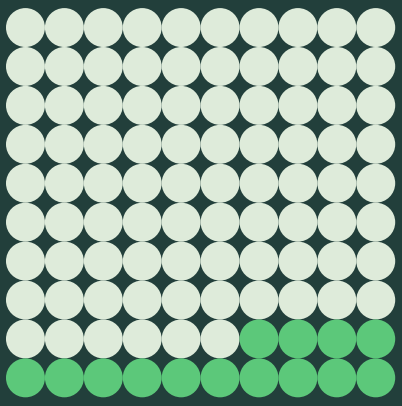
In the case of Oil and Gas companies, operating to ISO 31030 standards for over 20 years as common practice – their risk appetite is an intrinsic part of everyday culture, so they are less exposed. Other sectors are perhaps now catching up.

The future of ISO 31030 holds promise. As adoption continues to expand, it’s only a matter of time before it transitions from guidance to an industry standard. But regardless of whether compliance becomes a legal requirement or not, ISO 31030 sets a universal benchmark, signifying that now is the ideal time to integrate it into operational frameworks.

2. Weathering the storm

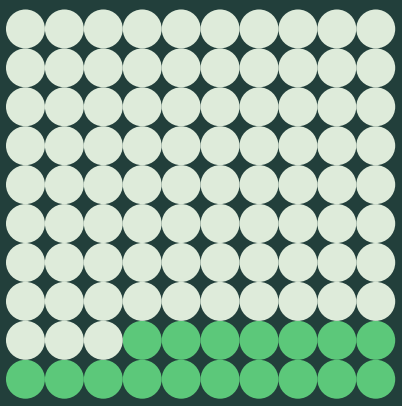
Extreme weather

76%
of organisations say that they have been directly affected by extreme weather



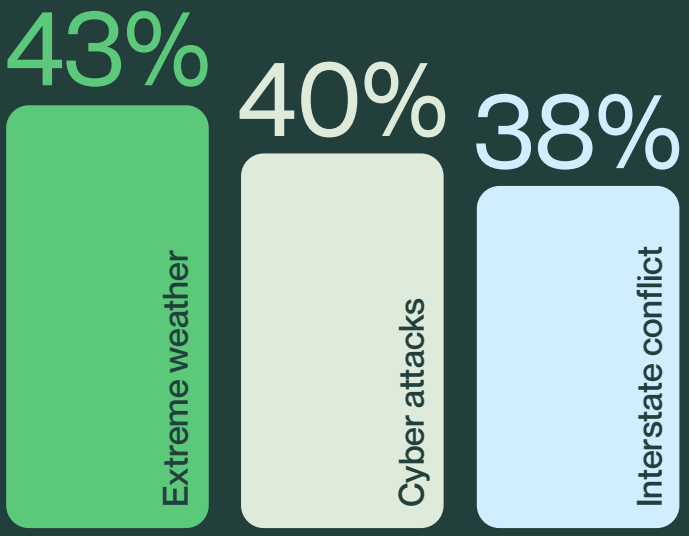
86%

The highest impacted industry is manufacturing where operations are dispersed amongst a large amount of physical environments and geographies



83%

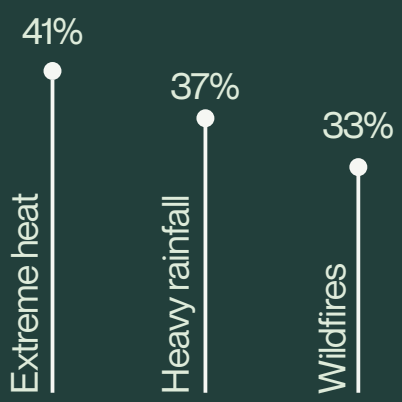
Media also ranked high in impact, which accounts for the risks involved in reporting on these extreme weather events at source



Biggest risk to operations by 2030

Risks that would have the most impact on their operations

Extreme weather events most concerning to organisations



However, when we looked to the future

25% said that they don't have plans in place to mitigate risk around climate or sustainability

Our research asked respondents to look at the risks they are most concerned about in the next two to ten years. There are certainly different risks highlighted between the two time-frames, but the second most concerned risk across both is natural disasters and extreme weather

A natural threat

We asked organisations what they considered to be the biggest risk to their operations by 2030. It was interesting, and somewhat surprising, to see that extreme weather is ranked first.

Numerous studies this year, including from PwC, have pointed to cyber security as the biggest operational risk keeping business leaders awake at night. Yet we are now seeing extreme weather perceived as the most tangible and long-term business risk.

The near constant reporting of wildfires and flooding across the world in the last twelve months will be a defining factor. From the wildfires of Hawaii and Canada, to the 50-degree Celsius temperatures in South America and flooding in China, many of the major events recently experienced in the world have been related to climate risk.

According to a study by Nature Medicine, nearly 62,000 people died of heat-related deaths last year during Europe's hottest summer on record.

As a global trend, the common theme of all climate-related risks is that they are indiscriminate and lead to tangible risks, whether physical risk to staff or operational risks such as infrastructure and supply chain disruption.

The tangibility of risks has a significant role in these figures too. Extreme weather has a more direct and immediate physical impact than a cyber attack, which may have economic and reputational risk but is unlikely to cause loss of life.

Although relatively closely matched

Extreme weather • 43%

Cyber attacks • 40%

Interstate conflict • 38%

are the top three concerns.

Close to home

Proximity also has a role to play. As extreme weather events continue to escalate, disasters are more likely to occur on our own doorstep. Personal experience is a sure-fire way to heighten awareness in global populations.

It is on the radar for companies now as it comes to the forefront of our own experiences. This is echoed in our research which found that almost three quarters (73%) of organisations say that they have been directly affected by extreme weather.

The highest impacted industry is Manufacturing (86%) where operations are dispersed across numerous physical environments and geographies. Media also ranked (83%) high in impact, which accounts for the risks involved in reporting on these extreme weather events at source.

Combine this more direct experience with the macro trends, extreme weather events and the devastating effects are only going to increase. We run the very real risk of failing to meet the United Nations goals of reducing emissions by 45% by 2030 and reaching net zero by 2050.

The heat is on

Of all the extreme weather events, the most concerning risk is extreme heat for 41% of organisations polled. The second and third biggest concerns are heavy rainfall and flooding (37%) and wildfires (33%).

This makes sense because not only can extreme heat affect personnel through conditions such as heatstroke and severe dehydration but it can also lead to associated factors related to extreme heat, such as wildfires.

Although extreme heat can be one of the easiest extreme weather risks to mitigate operationally, this can depend on operational environments and any extenuating circumstances. For example, extreme heat will cause a high demand for electricity for cooling systems, which can cause poor outages in certain locations and that could make it hard to mitigate the extreme heat risks for a company.

A bleak forecast?

We asked organisations to tell us the risks that would have the most impact on their operations and natural disaster came out highest (34%) ahead of societal/cultural (30%).

This fits with the other results we've seen from the report. However, when we looked to the future, 25% said that they don't have plans in place to mitigate risk around climate or sustainability.

This is concerning as we've already identified that it is one of the biggest risks on a macro level. What used to be latent and perceived as a longer-term risk, has now become a central part of business continuity plans. We are experiencing more immediate physical and direct operational impacts.

It is crucial that organisations begin to incorporate climate risk into day-to-day risk management plans, as the risks posed to personnel are becoming more tangible.

Our research asked respondents to look at the risks they are most concerned about in the next two to ten years. There are certainly different risks highlighted between the two time-frames, but the second most concerned risk across both is natural disasters and extreme weather.

'25% said that they don't have plans in place to mitigate risk around climate or sustainability.'

What do we take from this? You could say it shows an apathy and lack of confidence in resolving climate-related risks. Or you could believe that organisations now accept that this is a long-term issue. Our sense is that for the majority it is the latter and that there is an appetite for change, not just mitigation.

Climate risks cover a wide range of potential incidents, from extreme heat to deadly hurricanes, so there isn't a 'one-size-fits-all' rule for mitigating these risks. In general, organisations should ensure actionable and tested plans are in place for any potential extreme weather event, such as authoring evacuation plans, establishing primary and secondary methods of communication and ensuring personnel, assets and sites are equipped with the necessary protective equipment.

3. The information tsunami

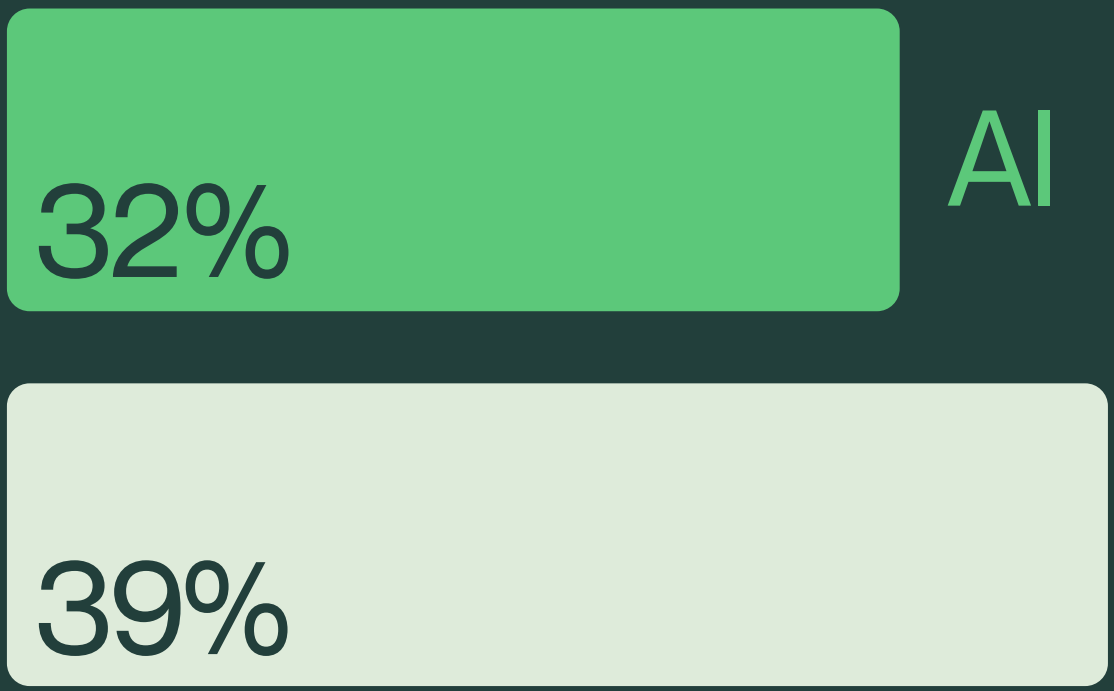
Artificial intelligence

Almost three quarters

72%

of those surveyed said that they are likely to integrate AI into their travel risk management process in the next six to twelve months

AI ranked as the second most utilised source of information related to business travel, after travel management companies



The rise of AI

As part of developing this research report, we were keen to take a look at the appetite and adoption of AI in travel risk management.

‘According to government research, around one in six UK organisations have embraced at least one element of AI technology already and our results echoed this trend.’

Almost three quarters (72%) of those surveyed said that they are likely to integrate AI into their travel risk management processes in the next six to twelve months. These are big numbers and the appetite is clearly there. Organisations want to use it, but the reality is that many just don’t know how as of yet.

The evolution of AI technology has been rapid in the last year, but the sense is that organisations are taking their time to make sure they are comfortable with integrating it into their processes. There is the reputational risk of using it too quickly and for problems to occur.

We are yet to see any high-profile failures resulting from the use of AI that might put the brakes on widespread adoption.

The prediction is that the fast pace of change will continue, but in the meantime, organisations are still figuring out the opportunities and the risks, in other words, the unknowns. Forbes UK research suggested that 42% of us are still wary of a dependence on AI and loss of human skills, and AI will need to be able to demonstrate another level of value before its adoption becomes commonplace.

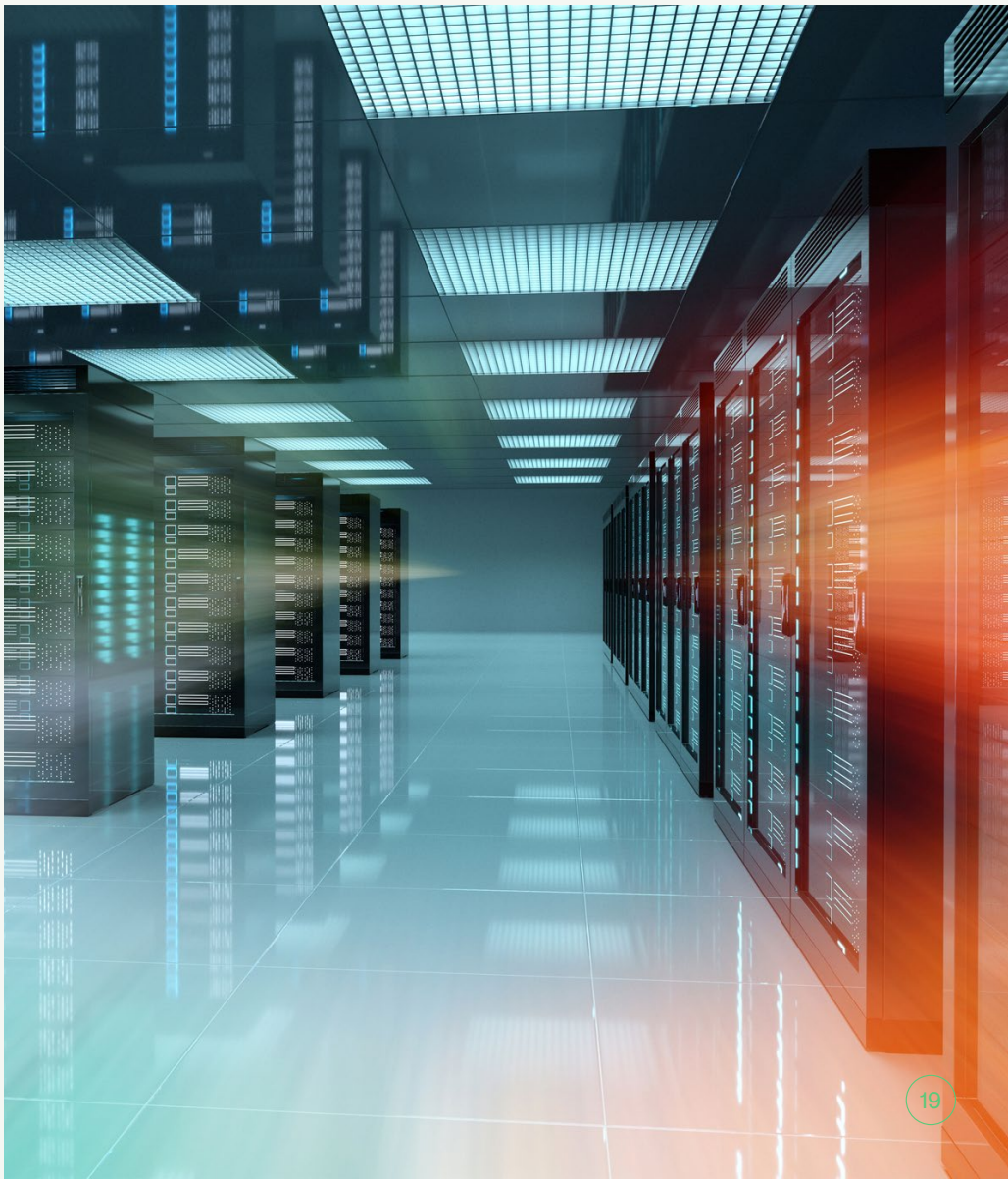
Trust vs risk

Much of the appetite in the last year has been built around the more ‘descriptive’ use of AI technology as an additional information source or a more sophisticated version of a search engine.

There’s minimal risk in using it as a search engine and it can be a very useful jumping off point for ideas and as one information source amongst others.

It is true to say that there is some risk however, in that information sources are not qualified. There is some unconscious bias too, borne out of the potential dataset limitations and sources. Nevertheless, there is limited risk to your organisation using it in this way.

Our research echoes this view, revealing AI (32%) as the second most utilised source of information related to business travel after Travel Management Companies (39%). In this question, AI also came out higher than third-party assistance providers, social media, government agencies, keyword alerts, news outlets and aggregators. Perhaps the most interesting observation here is that risk managers are preferring to use AI for intelligence gathering over government or news sources. Ease and speed of usage can account for its desirability, but it also demonstrates a level of trust already in AI as a valid source of intelligence.



Where's my data?

The promise is that we can move to a more 'generative' use of AI, where we could use it for process verification, right up to the development of automated risk management tools.

'In the 2023 budget, the UK government committed almost £1 billion of government funding towards AI research.'

But the stumbling block is around trust - 'generative use' of AI involves inputting data and that opens a Pandora's box of questions around how that data is being manipulated. What about GDPR and the security of servers? The UK and other overseas markets are also not prepared for these developments from a regulatory standpoint.

As we use AI more, the potential for distrust increases because the risks are greater. Only time will tell, but one surety is that it won't be long before we understand AI's full potential. Artificial intelligence tools are best used in conjunction with more traditional intelligence gathering, so that it can be verified using other sources to ensure accuracy and reliability. With the rise of generative AI, internal processes should be developed regarding the input of private or personal data and configuration of any AI-generated software.

4. Beyond borders

Regional insights

We asked respondents to identify the biggest risks for-

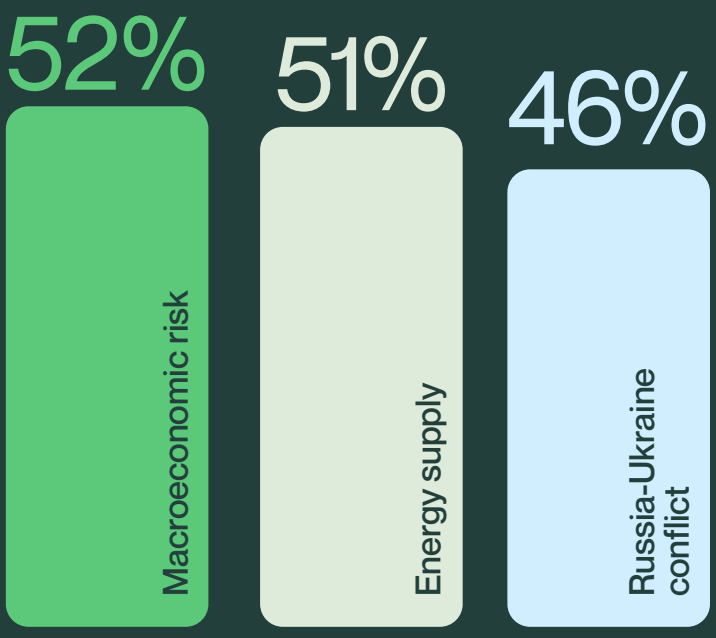
Middle East & North Africa (MENA) in the next 12 months:

53% geopolitical tensions

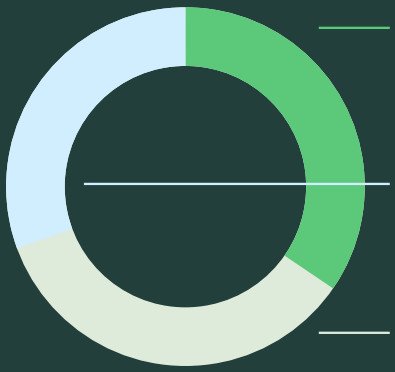
49% Islamist insurgencies

48% autocratic rule

Europe CIS in the next 12 months



Asia Pacific region in the next 12 months



50% food insecurity

44% North Korea hostility

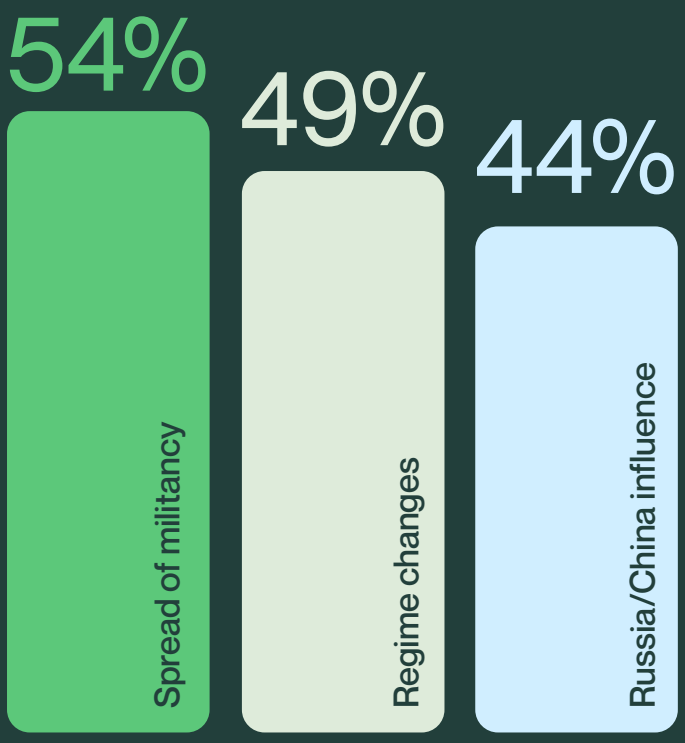
51% China/Taiwan tensions

The Americas in the next 12 months

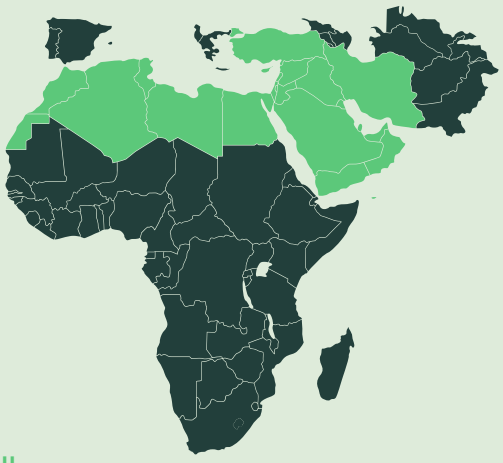
55% narcotics organisations

49% political violence & 48% corruption

Africa in the next 12 months



Middle East & North Africa



By Jacob Weiss,
Associate Analyst

We asked respondents to identify the biggest risks for Middle East & North Africa (MENA) in the next twelve months and geopolitical tensions came out top (53%), followed by Islamist insurgencies (49%) and autocratic rule (48%).

These results are not surprising, given regional developments over recent years. In previous years, we may have seen Islamist insurgencies receive a higher vote, but the decreased capabilities of groups such as al-Qaeda and Islamic State have reduced this perception of threat. Autocratic rule is also a constant when it comes to perceptions of risk in this region.

‘Deep and long-lasting political issues remain across the region’

These results were collected before the Hamas assault in Israel, a complex and destructive attack which has wide-ranging implications for civilians in Israel, the Palestinian territories and the wider Middle East. The emergent Israel and Hamas conflict contains elements of all three biggest risks for the MENA region.

Geopolitical tensions between rival MENA states can lead to obstacles to effective business practice at short notice, which is likely why diverse business sectors listed this as their biggest risk. Sanctions and restrictions on imports and exports can be imposed without significant forewarning, while conflicts and political instability can result in price spikes in commodities.

For Energy and Mining, it is unsurprising that Islamist insurgencies are ranked as the top risk. Al-Qaeda and Islamic State have energy infrastructure as a priority target for operations, likely due to their importance for state stability. This is the case in Algeria, which witnessed the large-scale al-Qaeda attack on the Tigantourine gas facility in Amenas in 2013, and Iraq, Syria and Egypt, which sees semi-regular attacks on energy infrastructure by Islamic State affiliated groups.

The ebb and flow of fast-moving political developments across the region often results in significant tensions between nations, occasionally bordering on outright hostility. While 2023 saw an ease in the Saudi Arabia-Iran rivalry, significant tensions remain that could derail the progress made in bilateral relations, not least any potential Iranian direction or influence over the Hamas assault in Israel.

Deep and long-lasting political issues remain across the region, including the status of the Palestinian territories in the aftermath of the Hamas-Israel conflict, political Islam and political schisms and conflict in Syria and Libya, which will continue to drive regional relations over the coming twelve months.

Europe & CIS

By James Towndrow,
Regional Intelligence Analyst (ECIS)

We asked respondents to identify the biggest risks for Europe CIS in the next twelve months and macroeconomic risk (52%) followed by energy supply (51%) and Russia-Ukraine conflict (46%) were ranked the highest.

The Russian invasion of Ukraine, adding to the residual impacts of the Covid-19 pandemic, is the main driver underlying the risks facing organisations across Europe. High energy prices and slowed economic growth, traceable to the conflict, demonstrate the capacity for major geopolitical risk factors to disrupt global supply chains and impact consumer spending. Widespread economic and political impacts associated with the conflict have forced governments to adopt tighter monetary policies, in turn prompting the reconsideration of existing climate goals.

High inflation slowed economic growth, and the increase in interest rates as a result of wider geopolitical risk factors is likely to undermine investor confidence. Impacts are likely to be felt in sectors including manufacturing and construction. The current trajectory of fighting in Ukraine points to a protracted conflict. European sanctions against Russia have dented but failed to derail the Russian economy, with the Kremlin orientating spending with a view to sustaining military operations in Ukraine well into 2024 and likely beyond.

Domestic governments are likely to orientate policy towards navigating further economic turbulence over the coming winter. Concerns regarding supply drops in the availability of Russian natural gas, increased global demand for liquefied natural gas (LNG) and the possibility of more severe winter conditions in Europe add to continued uncertainty ahead of the upcoming winter.

Americas

By Felipe Wagner,
Threat Analyst (Americas)

We asked respondents to identify the biggest risks for the Americas in the next twelve months and the influence of narcotics organisations (55%) followed by political violence (49%) and then corruption (48%) was the top three ranked.

Narcotics organisations are the main risk as precedent suggests their operations are liable to pose a direct risk to lives either through targeting rival criminal groups, the security forces, or civilians in cases of indiscriminate violence.

The risks associated with political violence take place amid election cycles that rely increasingly more on social media for exchanging information, which leads to further polarisation, dissemination of fake news and organised protests.

Corruption remains a priority risk as countries in the region face challenges to develop efficient methods of accountability and checks-and-balances systems. The problem is accentuated by slow and inefficient judicial systems and limited economic growth, which means that politicians and low-level bureaucrats are more likely to take risks.

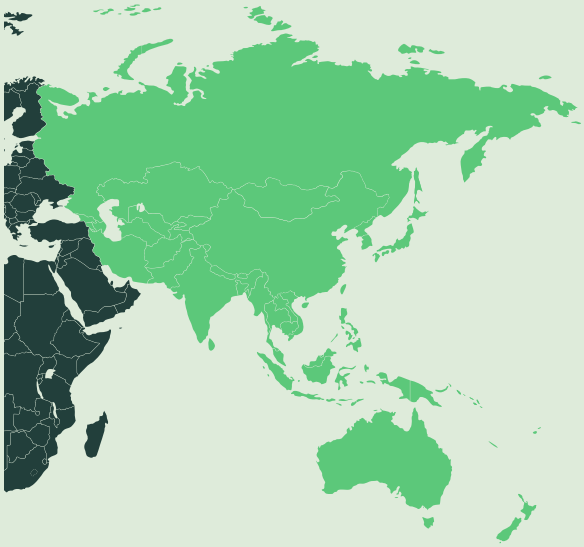
The presence of drug-related violence increases kidnapping rates and criminality. The security forces are commonly under-equipped and badly trained, which means that narcotic groups can extort the local population with minimal resistance. Their influence and power will grow as their main source of income - drug trafficking - is unlikely to decrease.

A deterioration of the security risk environment in Ecuador is likely to destabilise the region. The country's strategic location along drug smuggling corridors that come from Peru and Bolivia and continue through Colombia and Central America means that turf wars will increase.

Energy companies in the Americas, particularly in Mexico, consider narcotic groups their biggest risks as oil theft continues to occur in the Red Triangle region. Media companies understand the risks posed by these organisations as investigative journalists are liable to be assassinated. As these groups control vast territories in isolated areas, media companies will require dedicated security support to film or study animals/plants in high-risk regions.

Asia Pacific

By Aushaz Irfan,
Intelligence Analyst (APAC)



We asked respondents to identify the biggest risks for the Asia Pacific region in the next twelve months and food insecurity (50%), China/Taiwan tensions (47%), North Korea hostility (44%) were the top three ranked.

Food insecurity in the Asia Pacific region has been significantly exacerbated due to the impacts of the Ukraine war and the increased propensity of climate-induced disasters and extreme weather events. Even though an escalation in the Taiwan Strait and the Korean Peninsula is unlikely to materialise, heightened tensions can pose operational risks to businesses in the region due to their potential impact on supply chains and regional trade.

Key drivers of food insecurity in the region include rising global food prices, increased fertiliser and fuel prices, supply chain disruptions, devalued local currencies and limited capacity for social safety nets, following slowed economic growth after Covid-19.

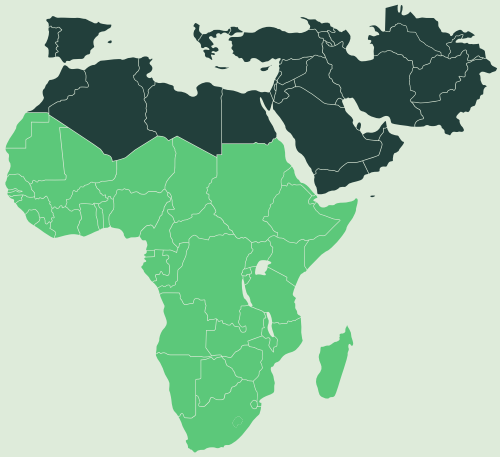
Extreme weather events, such as floods and droughts, have increased in frequency and exacerbate the problem due to their detrimental effect on crop yields and harvesting, livestock and agricultural infrastructure.

Countries most at risk of food insecurity include Afghanistan, Bangladesh, Laos, Myanmar, Pakistan, Sri Lanka and the Pacific Islands, mainly due to their socio-economic environments, dependence on agriculture and exposure to climate-induced natural disasters. The increasing food insecurity risks in APAC are likely to increase supply chain disruptions and deteriorate political stability in affected regions due to the propensity of food insecurity to lead to political violence.

Elsewhere, China has significantly increased its military activities in the Taiwan Strait, with unprecedented daily incursions by Chinese aircraft near Taiwan. The persistence of provocative actions by North Korea, combined with the increasingly defensive responses by South Korea and Japan, highlights a deteriorating trend in the Korean Peninsula.

Africa
(ex. North Africa)

By Tess Daniel,
Senior Security Analyst



We asked respondents to identify the biggest risks for Africa in the next twelve months and the spread of militancy (54%), followed by regime changes (49%) and Russia/China influence (44%) were the top three ranked.

The spread of militancy in Africa has been evident in the past year with a marked 68% increase in fatalities involving civilians. The militant Islamist threat is not monolithic but comprised of over a dozen different militant groups operating largely within the Sahel and Somalia. In the Sahel, the Islamist violence has rapidly expanded in casualties and geographically, spreading from Mali, Burkina Faso and Niger into neighbouring countries such as Ghana, Togo and Benin.

The past year has seen a continuation of the trend of military takeovers that started in recent years. Since 2020, there have been ten attempted coups, mostly in West and Central Africa, underscoring a rapid undoing of democratic systems in the region. This is largely reflective of long-standing frustration with civilian leaders in Africa. Several countries are now ruled by transitional military authorities, including Burkina Faso, Chad, Gabon, Guinea, Mali, Niger, and Sudan.

Meanwhile, long-standing international partners, such as the United States and France, have lost some of their influence in Africa to the benefit of new partners such as Russia. With the help of the Wagner mercenary group, Moscow is successfully inserting itself in countries such as Mali and Burkina Faso and is taking advantage of Western policy missteps, growing anti-European sentiment, and long-standing failures of international and local actors to address the root causes of regional instability.

The three identified risks are interrelated, as most of the political instability that preceded regime changes was linked to deteriorating security situations amid the spread of militancy. The series of coups and the growing influence of authoritarian governments like Russia and China is indicative of a broader global turn away from democracy. The expansion of militant threats, combined with political instability and the influence of Russia, is creating growing operational risks for companies with a footprint in the Sahel.

‘The past year has seen a continuation of the trend of military takeovers that started in recent years.’

5. Tackling the elements

Monitor the risk environment

Relevant, corroborated and up-to-date information plays a key part in effective risk identification. Stay abreast of the latest developments using data from multiple reliable sources, and be wary of misinformation. External suppliers or embedded analysts can be valuable for managing the collection and analysis of intelligence, identifying new or evolving risks and monitoring long term trends on your behalf, where you may lack the in-house resource.

Prepare with crisis management planning & training

This should involve forecasting potential crises specific to your organisation and developing plans around how to deal with them. The process includes the identification of the characteristics of a crisis and subsequent intervention in order to minimise reputational, financial, operational or legal risks and facilitate recovery.

Mitigate global risks to staff and operations with travel risk policies

When we write travel risk policies, we account for your business culture, risk tolerance, operational footprint, countries of travel and management framework, and provide a travel risk policy unique to your organisation. The policy and recommendations consider the three stages of travel: before, during and after, and are informed by a thorough review of risks that your workforce could be exposed to.

Get ahead of location-specific risks by planning your evacuation and emergency responses

It is essential to develop comprehensive plans to extract your staff from challenging operating environments. Your plan should look at your staff exposure, infrastructure, routes, ports of departure, operational issues, and the escalation point 'triggers' that signal a deterioration in the specific environment.

Ensure robust planning around staff travel

Leveraging ground support and protective services ensures the safety of your staff, executives and loved ones to enable them to travel with confidence. It is important to assess the threat and risk environment, and find solutions in an individualised security plan, scaled to accommodate your different environments and risk appetites.

Take steps towards mitigating personalised risks

Building a personalised risk profile requires a strong bond of trust between business and traveller. In order to make sure risk profiles are robust and effective, businesses must find honest and transparent ways to gather sensitive personal information from employees, while making every effort to keep that information secure and prevent it from falling into the wrong hands. This process, while complex, is crucial to ensuring that each traveller is equipped with the knowledge and resources they need to navigate their own unique risk experience.

High risk doesn't have to mean dangerous territory

With the right risk management partner, you can safeguard the health and wellbeing of your people in every corner of the world.

At Healix, we work with organisations to proactively mitigate risks before they happen and expertly manage them when they do, protecting your people, organisations and assets wherever they are.

Whether your focus is on creating a resilient, ISO 31030 compliant organisation, or delivering on growth and opportunity, Healix can help.

Discover more about how we can support you

enquiries@healix.com

healix.com

Head office
Healix

Healix House
Esher Green,
Esher, Surrey,
United Kingdom
KT10 8AB

USA
Sales Office

HX Global
300 Wildwood Ave,
Suite 250,
Woburn,
MA, 01801

UK
Operational Office

Healix Health
5th Floor, 3 Temple Quay,
Redcliffe, Bristol,
United Kingdom
BS1 6DZ

Canada
Operational Office

Healix International
701 West Georgia Street,
Suite 1501,
Vancouver,
B.C., V7Y1C6

New Zealand
Operational Office

Healix New Zealand
Suite 8,
40 Arrenway Drive,
Rosedale, Auckland,
0632

Singapore
Operational Office

Healix International
143 Cecil Street,
GB Building #03-01,
Singapore,
069542

South Africa
Operational Office

Healix International
CMA Office and Conference
Park, No 1 Second Road,
Halfway House, Gauteng,
1685