echo

INTERNATIONAL SOS

# RISK OUTLOOK 2026

Leading through uncertainty, shaping the pace of preparedness.

WORLDWIDE REACH. HUMAN TOUCH.

internationalsos.com

# Contents



# Foreword

**2026 begins in a world where volatility is no longer the exception—it is the operating environment.** Risks intersect, disrupt, and escalate faster than traditional planning cycles can absorb. In this reality, preparedness moves from being a defensive posture to a strategic advantage. It becomes the cornerstone of organisational confidence, continuity, and long-term performance.

Risk Outlook 2026 draws on more than 40 years of supporting organisations in moments of complexity and transformation. This year's global survey of risk leaders delivers a clear message: those who anticipate, adapt, and act with speed are the ones who protect their people, sustain their operations, and strengthen their competitive edge.

Organisations today are navigating a convergence of pressures: geopolitical fragmentation, natural hazards, rising costs, and increasing polarisation. Trust is being tested as misinformation grows more sophisticated. And the strain on employees—particularly regarding mental health—continues to intensify. Human capital has never been more strategically important, or more vulnerable.

In this environment, preparedness must be intelligent, dynamic, and continuous. Artificial Intelligence has become a critical force multiplier, enabling real-time risk detection and faster decision-making. But technology alone cannot replace judgment. The integration of advanced analytics with deep human expertise is what delivers clarity from complexity—and transforms uncertainty into actionable foresight.

At International SOS, our mission is to empower organisations to operate anywhere with confidence. Whether entering new markets, managing remote operations, or responding to sudden disruption, we stand alongside leaders to enhance resilience at every stage. Our commitment is simple: protect your people, support your continuity, and help you lead responsibly amid accelerating global change.

As you explore this year's Risk Outlook, I encourage you to view risk not as an obstacle, but as a catalyst for stronger resilience and smarter leadership. With the right preparation, trusted intelligence, and effective partnership, uncertainty becomes navigable—and your organisation can not only endure, but thrive, in the year ahead.

**Arnaud Vaissié**
Co-founder, Chairman &
Chief Executive Officer

*"This year's global survey of risk leaders delivers a clear message: those who anticipate, adapt, and act with speed are the ones who protect their people, sustain their operations, and strengthen their competitive edge."*

# Research process

**2026 Risk Outlook** is the result of detailed analysis from four pillars of International SOS proprietary research and expertise. **These are:**

1. **International SOS Security and Medical experts' views**
2. **Business Resilience Trends Survey**
3. **Security & Medical risk ratings**
4. **On-the-ground global health & security network**

## Security and Medical experts' views

International SOS draws on some of the world's foremost experts in security and health to support clients, and inform its strategy, planning and operations. Our elite team includes former military operatives, intelligence analysts, logistics specialists and medical professionals.

Interviews were carried out with members of our International Security Advisory Board[1] and senior health and security leaders within International SOS in October 2025. Their insights, quoted throughout this report, validate and add depth to the findings of the Business Resilience Trends Survey.

## Business Resilience Trends Survey

The 10th edition of the Business Resilience Trends Survey, carried out in September 2025, uncovers the views of 860 business leaders responsible for workforce health and security and organisational risk management. The Survey explores how organisations around the world perceive and mitigate new and existing health, wellbeing, and security risks for their employees, particularly those working abroad.

***The survey examines:***

- **Perceptions of the changing risk landscape**
- **Strengths and gaps in corporate provision**
- **Expectations for the coming year**

## Security & Medical risk ratings

Security risk ratings reflect the risk to employees from criminal activity, political violence (including terrorism, insurgency, and war) and social unrest (including, sectarian, communal and ethnic violence) as well as violent and petty crime. Other factors, such as the robustness of the transport infrastructure, the state of industrial relations, the effectiveness of the security and emergency services and the country's vulnerability to natural hazards are also evaluated. A single security risk rating is assigned per location. However, risks can vary greatly within a country's borders and so more granular ratings are available, as well as details of the primary risk factors influencing these ratings.

These ratings are updated annually and represented on the openly accessible International SOS Risk Map[2]. All clients with access to Quantum can view live risk rating updates to a city risk rating level. Our risk ratings are proprietary, developed over many years, and based on access to information that is not publicly available.

Medical risk ratings are determined using a proprietary algorithm with over 20 internal and external data points, and the first-hand knowledge of our specialist medical professionals. The selected data points reflect a range of health risks and mitigating factors, including, but not limited to: access to and standard of emergency services, outpatient and inpatient medical care, medical evacuation data, quality of pharmaceutical supplies,

infectious disease risks, access to improved water and sanitation, environmental risk factors, security risk rating, and cultural, language or administrative barriers.

The medical landscape can vary widely within countries. For example, major cities may have better access to quality medical care, whereas remote or rural locations may have limited availability of health facilities and specialist care. An overall single rating is given at a country[3] level (clients also have access to ratings for selected cities and a subset of the factors used in determining the risk ratings).

## On-the-ground health & security network

**International SOS has health and security experts based in more than**

**1,200 locations in 90 countries.**

This Risk Outlook report is complemented by more in-depth regional reporting available exclusively to our clients The regional assessments are developed by our lead area analysts, who have deep local experience analysing risks, threats and hazards and supporting clients in the field.

1. https://www.internationalsos.com/experts-security
2. https://www.internationalsos.com/risk-outlook
3. The term 'country' refers to traditional countries or independent states, as well as other geographic entities including dependencies, territories and areas of special sovereignty.

**On behalf of International SOS, Echo Research carried out online interviews with**

**860 senior risk decision makers responsible for the health and security of:**

- Employees
- Contractors
- Students and faculty
- Other people within the organisation

**Across 94 countries**

**8%** Middle East

**27%** Europe

**25%** Asia

**21%** Americas

**12%** Africa

**7%** Oceania

# Key authors

## Dr Irene Lai

*MBBS (Sydney) FFTM RCPS (Glasg),*
*Global Medical Director, Medical Information & Analysis, International SOS*

Irene has over 20 years' experience in health intelligence, risk assessment, communications, and clinical medicine. Her focus areas are emerging and pandemic health threats, heat and climate impacts, travel, public health, and emergency preparedness and response. She trained primarily in internal medicine, working in Sydney, Chicago, and New York. She has held a range of senior roles within the Group, in Singapore, Jakarta, and Sydney.

## Cvete Koneska

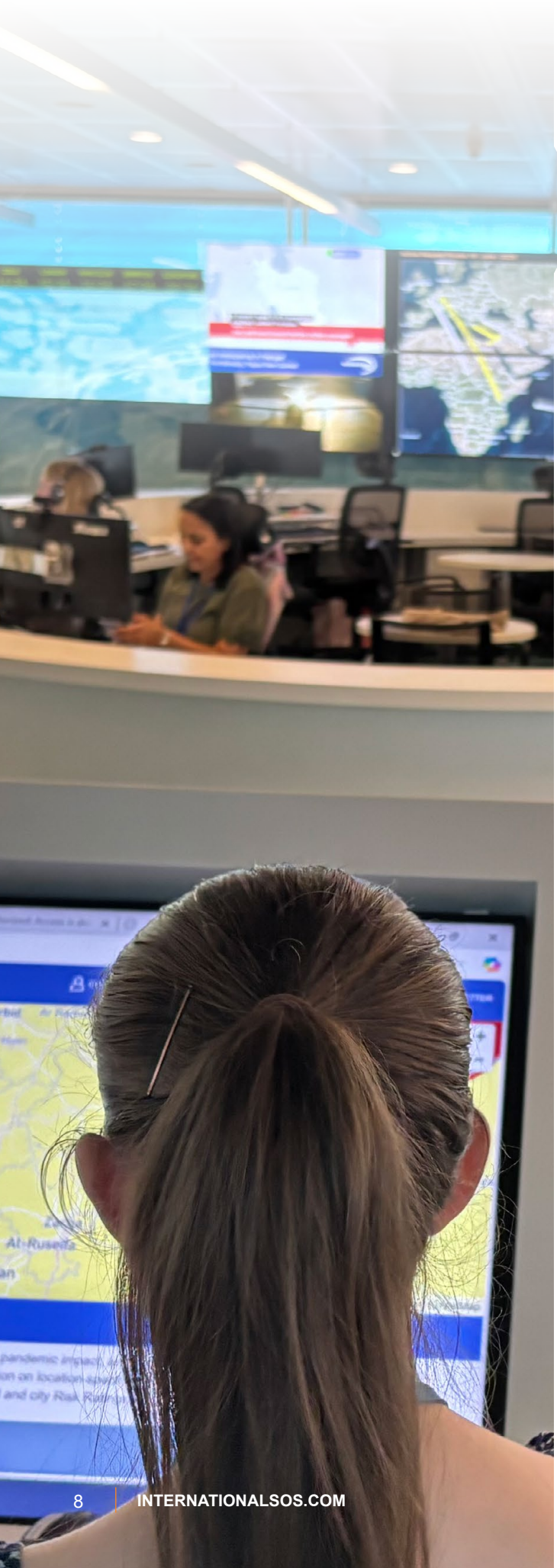
*Global Security Director, International SOS*

Cvete has over 15 years' experience in security intelligence, geopolitical risk analysis and leading high-performing analyst teams. She directs International SOS' global security analysis function, delivering timely, actionable insights for organisations operating in complex and high-risk environments. Her expertise spans geopolitics, operational risk and strategic decision support. Cvete has held senior roles within the risk and intelligence sector and is a recognised thought leader, contributing to academic and industry publications. She holds a bachelor's in Political Science and International Relations from the American University in Bulgaria, a master's in Politics, Security and Integration from University College London, and a Doctorate in Politics from the University of Oxford.

## James Wood

*Regional Security Director, International SOS*

James has over 15 years' experience in security consulting, travel risk management, crisis and escalation management, and business continuity. He leads security strategy and support for clients across Northern Europe. Prior to this, he led International SOS' global Security Consulting Practice, managing expert teams and client engagements worldwide. James began his career as a police officer with Thames Valley Police, UK, and holds a BA (Hons) in French and History from the University of Warwick. He is a certified Business Continuity professional and a member of the Security Institute and the Business Continuity Institute.



# Risk at full tilt

The **fragmenting world** we warned about in last year's Risk Outlook fragmented at speed and from a multitude of angles.

## Risks emerging faster than organisations can deal with

***Agreement with statements on organisational risk environment***

**80**

Being able to detect risks quicker would give us a competitive advantage

**74**

The timescale for making critical risk decisions is getting shorter

**58**

We are equipped to monitor risks in real time or near real time

**57**

New risks are emerging faster than we can deal with them

***Speed of organisational response to new risks***

The geopolitical shifts over the past 12 months have left many organisations running to catch up with a new world order, while also dealing with a rapid acceleration of security and health challenges.

Extreme weather events, new conflicts and fresh developments in existing ones, social unrest and cyber threats, all come with increasing frequency. Time is on nobody's side; new challenges emerge at a speed that leaves many businesses feeling blindsided.

# 57%

**Almost six in 10 respondents in our global Survey say new risks are emerging faster than they can deal with them.**

The increased pace makes new demands on risk management professionals. *"CSOs have to be more agile to be able to shift quickly to address new and unexpected risks,"* says International SOS Senior Security Adviser, France, Christophe Suptil.

As the velocity of threats rises, the speed at which organisations can identify and react to them becomes a differentiator between those who thrive in a complex risk environment and those who just manage to survive. Respondents to our Survey agree;

# 80%

**say that being able to detect risks more quickly would give them a competitive advantage.**

The capacity to verify risk information at speed is rated as the most critical factor in responding to new risks by respondents, but only one in five (20%) believes they are capable of doing so.

Anticipating new risks and having access to time-sensitive risk intelligence were identified by respondents as the areas of highest importance where they had least confidence in their performance. They highlighted organisational culture, procedural complexity and information overload as brakes on their ability to respond, as well as resource constraints.

*"Businesses can do absolutely nothing to affect how quickly things happen, but what they can do something about is their ability to prepare better, to anticipate change."*

**Cvete Koneska,**
International SOS Global Security Director

# More with less

Although almost two-thirds of respondents to our Survey **(64%) say security risk has increased** in the past 12 months and **43% say health risks have intensified** – with similar proportions expecting increases in 2026 – they have to manage the risks with flat or reduced resources.

One in ten security and health specialists anticipate budget cuts next year, and around two-thirds (66% of security specialists and 68% of health experts) say their funding will be static. One Middle East-based risk management and insurance specialist said their greatest security challenge was *"Taking on more initiatives and business growth with the same number of resources."* A senior medical officer in the same region warned that *"Lack of resources and budget will further compound an already fragile workforce."* Security and health specialists must ensure executives are well briefed about the range and extent of risks their businesses are facing.

Despite the intense focus on artificial intelligence (AI) as a route to greater efficiency, our Survey shows that security teams are not yet confident in its reliability.

**Only 6%**
**rank AI as an important factor in helping them manage risk.**

This suggests security functions may be under-utilising new data-filtering and pattern-finding tools that - providing there are humans in the loop to verify the results - could save them time and money. Overall, the budgetary constraints leave around three-quarters of security and health specialists trying to do more with less, or frozen, funding. It's a significant spur to developing new ways of working.

*"You can drive efficiency in risk management without cutting quality, by being more agile and using technology and partnerships to push improvement."*

**Dr Katherine O'Reilly,**
International SOS Medical Director

## So what?

Businesses need to develop the agility and reliable information sources to be able to decode and prioritise the "weak signals", early signs of a security threat, or the threshold at which a health risk demands action. However, they also have to be able to close down unfounded, incorrect or inaccurate rumours of security or health threats.

Risk management teams need instant access to reliable intelligence that helps them judge the right time to act, to find the right balance between disrupting the business unnecessarily and being caught out by restrictions or unmanageable risks to employees.

Critical Event Management (CEM) relies on regularly updated systems and risk registers for the highest-severity threats, together with playbooks that let teams respond efficiently and effectively, a vital capability for security and health specialists working with limited resources.

Intelligence-led planning and anticipation will be vital in 2026, but so will rapid response; the window of opportunity to react and protect workforces has narrowed. Three-quarters of the security and health specialists in our annual Survey (74%) say the timescale for making critical risk decisions is tightening, but only around one in three (35%) is confident they can mobilise teams rapidly in a crisis. When hours can make the difference between a successful and an unsuccessful operation, organisations cannot afford to learn how to respond in real time.

As the pace of events quickens, organisations need confidence they are primed to identify relevant risks early and to act decisively to contain them.

# Everything at once

Where once security or medical teams had the chance to stop, to draw breath and absorb the lessons of an incident before they faced the next one, they no longer have that luxury.

New threats are increasingly overlapping, coming in waves to stretch organisational resilience and capacity to respond. The top issues cited by organisations as disruptors in our Survey include geopolitical tensions, cyber-crime, economic instability, employee mental health risks, economic instability and trade disputes. None of these is mutually exclusive or sequential.

The main internal resource that businesses depend on to face fast-developing threats is their people. But many employees report that their responsiveness and resilience have been worn down by successive challenges, including the pandemic and high inflation. They are also increasingly expressing underlying anxiety about the same global risks their employers must manage, including extreme weather events and discussions around nuclear incidents.

Organisational challenges also increasingly have more than one facet. *"There used to be some crises that were purely security issues,"* says International SOS Global Medical Director, Irene Lai, *"and medical teams weren't necessarily required in those crisis management meetings. Now there is rarely an event where we do not need representation from both teams."* As the short-term security risk is controlled, health aspects can come to the fore, or the two may emerge concurrently; respiratory conditions in the wake of wildfires or post-traumatic anxiety after evacuations.

**49%**

**of the risk and security specialists surveyed say the interconnectedness and convergence of risks have increased in the past 12 months.**

## Drivers of uncertainty in the global risk landscape

### Top 10 factors:

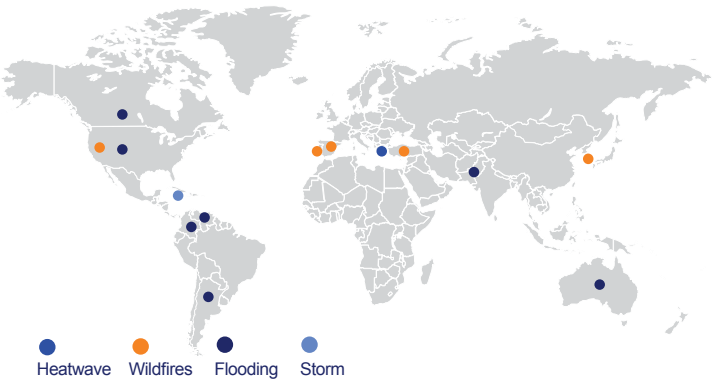
# Storms ahead

**Extreme weather** is an example of a threat that fuses security and health risks. Hazardous weather events have featured in previous Risk Outlook reports, but as their frequency increases, it becomes more urgent for businesses to account for them in security and health risk planning.

Extreme weather varies by region. In 2025, Greece suffered a record heatwave with temperatures topping 45°C. The associated wildfires were mirrored on the US West Coast, in South Korea, Spain, Portugal and Türkiye. Floods in Argentina, Pakistan, Colombia, Venezuela, Canada, Australia and many US states, cost lives and devastated property. In the Atlantic hurricane season, Category 5 storms caused devastation on the US East Coast and Jamaica.

There are both immediate and long-term security risks associated with hazardous weather events. In the immediate period before, during and after an extreme weather event, there are likely to be significant life safety risks accompanied with disruption; inaccessible support structures (such as communications, transport, supplies emergency services); and challenges to local authorities to manage and mitigate the risks. Longer term, more frequent and geographically disparate extreme weather events create direct and indirect challenges, including crop failures, food price inflation, socioeconomic deterioration, protest activity and mass migration. All these factors will impact the security risk landscape in a given country.

Alongside this, resource pressures created by extreme weather events can be a driver of instability and inter- and intra-state conflict.



# Heat of the moment

The 2025 report of Lancet Countdown on **health and climate change** highlights the dangers of extreme heat.

The higher temperatures and the increasing size of vulnerable populations have led to a

**63%**

**increase in heat-related deaths since the 1990s, reaching an estimated 546,000 yearly deaths on average in 2012–21.**

*"Almost half of the global population and more than one billion workers are exposed to high heat episodes and about a third of all exposed workers have negative health effects. However, excess deaths and many heat-related health risks are preventable"*[4].

Measuring ambient temperature is no longer enough to assess the risk to the workforce, with the Wet-Bulb Globe Temperature (WBGT) a better measure of heat stress on people. We expect to see more regulations regarding working in heat[5]. Employers will not be able to rely on air temperatures alone to guide them when to adjust work activities. They must have extreme heat policies and associated action which comply with these evolving regulations. Adaptive responses need to be thoroughly assessed for additional risks, such as floodlit night work in agriculture to avoid extreme heat bringing its own safety challenges.

Vector-borne infectious disease transmission potential increases with warmer temperatures. Clusters of mosquito-borne diseases, including dengue fever, Zika and malaria have appeared in locations where they are not usually present, such as the United States, Italy and France, sparked by travellers importing the virus and local environmental conditions being conducive to onward transmission.

By some measures, air pollution reached a record high in 2024, with sand and dust storms contributing significantly. 2024 also saw a record area of land affected by extreme drought[6]. According to the United Nations, approximately half of the world's population currently experiences severe water scarcity, a problem which is expected to grow[7].

*"I think extreme weather impact on health and security is going to continue to become a more salient topic,"* says International SOS Global Medical Director Dr Myles Druckman.

While other priorities have eclipsed the prospect of another pandemic for many organisations, global health experts remain vigilant. Funding changes to some public health surveillance agencies and international NGOs could lengthen alert times in the event of a future outbreak. Alterations to international aid allocation also affect programmes to suppress diseases, such as tuberculosis, raising the health risk for travellers and assignees.

*"We have become reliant on knowing that response will take place, and many outbreaks will be quashed before they become significant".*

**Dr Ryan Copeland,**
International SOS Regional Medical Director, Assistance, EMEA.

4. Ebi, K.L et al, 'Hot weather and heat extremes: health risks', Lancet, 398(10301), pp. 698–708. Available at: https://pubmed.ncbi.nlm.nih.gov/34419205/
5. National Weather Service, Wet Bulb Globe Temperature vs Heat Index. Available at: https://www.weather.gov/ict/WBGT
6. Romanello, M et al, The 2025 report of the Lancet Countdown on health and climate change. Available at: https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(25)01919-1/abstract
7. United Nations (n.d.) Water – at the center of the climate crisis. Available at: https://www.un.org/en/climatechange/science/climate-issues/water

# Forgetting health, forgetting the human

Health crises typically **develop over years**, shaped by local, national, and international health systems, supply chains, workforces, and societal behaviours.

This slow evolution can foster complacency, a trend compounded by post-pandemic confidence and reduced attention to health issues. In some countries, investment in community health systems and healthcare workforces has slowed, with resources prioritised elsewhere. Our Survey shows that health concerns currently rank well below security issues in shaping organisational risk uncertainty. And although data shows the burden of mental health issues continues to trend upwards, with an estimated more than one billion living with mental health conditions,

**mental health only rates in the top three concerns for**

**17%**

**of those surveyed.[8]**

International SOS case data indicates anxiety and stress are the most common mental health conditions requiring our assistance, with medication issues often complicating travel.

In response to the question in our Survey about the greatest health challenge facing their businesses in 2026, one health, safety and environment leader in Oceania identified *"Psychosocial risk management, especially aspects such as burnout and fatigue as related to job demands."* Where once such issues mainly were reserved to higher-wage economies, International SOS now receives requests for support with employee mental health and wellbeing from companies based in Africa and Asia.

At the global level, inequality in health outcomes is rising. Wealthier populations in high-income countries are better able to access scientific and technological advances aiming to extend life spans well beyond 100 years, while preventable conditions, including acute hunger, malnutrition, malaria, and cholera, continue to increase in other regions. As antimicrobial resistance grows, rendering existing antibiotics ineffective, without new ones arriving to replace them, bacterial diseases become more difficult to treat and outbreaks to contain.

*"Over the past five years, several factors have pushed a lot of people to consume less healthy, ultra-processed food,"* notes Dr Ahmed Fahmy, International SOS's Regional Medical Director, North Asia.

*"My concern is about malnutrition, not in the sense of not having enough calories, but just having bad diets, which links to non-communicable diseases[9]."*

Fatigue, distraction and at worst, burnout, erode productivity but also organisational resilience. *"Employers increasingly realise this is not an HR issue anymore, it's a strategic risk,"* says International SOS' Global Medical Director Dr Philippe Guibert. Workforce capability is also impacted by the more gradual effects of demographics and lifestyle on health in higher-wage countries. An ageing working population and rising levels of cardiovascular conditions and Type 2 diabetes are slow-burn risks that weaken business resilience.

Meanwhile, advances in technology, particularly generative AI, are changing the role of humans in essential services, with Bill Gates foreseeing that we will not need humans for most things[10]. Overreliance on technology risks eroding skills and human capacity in critical areas, including healthcare. Just as previous technological revolutions reshaped work, future innovations may alter how essential services are delivered, underscoring the need to retain human expertise alongside automated systems. Organisations need to ensure they have robust governance and are examining the long-term risks of adopting generative AI solutions.

## So what?

Expecting to be fighting on more than one front has to become standard corporate thinking. Organisations need to break down siloed mentalities; develop joint capability and joined-up thinking between security and medical teams. Coping with multifaceted threats and with multiple issues at once is likely to test internal resources beyond capacity; true resilience depends on choosing partners who can take up the strain when needed to ensure a proportionate response. Foresight over the risks that could eventuate at once and working out how to manage them is important. *"What if…?"* scenarios need to include the potential for simultaneous threats. But businesses cannot pause trading while they rehearse and prepare for all eventualities. *"You can't plan for every risk now,"* says James Wood, International SOS Security Director, Northern Europe. *"The most agile organisations are the ones that have an agnostic methodology, they can apply across multiple different factors."* What is critical is that everyone in an organisation, from CEO to receptionist, is clear about their role in a crisis and has developed the muscle memory through practice to respond as needed.

Though many organisations still have a way to go in adjusting to the complex present, one positive effect of the multiple disruptions of recent years is that they have had what International SOS Senior Security Adviser Dave Komendat describes as a "forcing function", improving organisational response.

*"Crisis management teams have been exercised almost continuously, it's a learned and practised skill set."*

**Dave Komendat**
International SOS Senior Security Adviser


8. World Health Organisation, World Mental Health Atlas 2024. Available at: https://iris.who.int/server/api/core/bitstreams/5897b3c7-2848-47a7-ba22-0a7902342a81/content
9. Santoro, C (2025) The high cost of healthy: How grocery prices shape American diets and health, AJMC. Available at: https://www.ajmc.com/view/the-high-cost-of-healthy-how-grocery-prices-shape-american-diets-and-health
10. NBC (2025). The Tonight Show. Available at: https://www.youtube.com/watch?v=uHY5i9-0tJM

# Fatal bytes

Remote attempts to breach corporate IT systems have become **one of the biggest security worries for all businesses**. State and non-state actors probe company networks for vulnerabilities to exploit.

**The US government's Cyber Intelligence Threat Integration Center tracked**

**2,593**

**ransomware attacks worldwide in 2024, up 15% on 2023 after doubling the year before[11].**

High-profile attacks in 2025, such as those, highlight the levels of organisational disruption and reputational damage wrought by infiltration and threats to restrict access to vital data or publish confidential records online. Cyber-crime was the second-highest rated factor driving risk uncertainty among our Survey respondents. Increased mobility and location-independent working add potential porosity to company networks. Cybersecurity challenges for staff travelling to all parts of the world with mobile devices is cited as the most significant security risk by a mobility and travel specialist in our Survey.

Corporate protection has evolved rapidly, but the techniques employed by bad actors in this space have become more sophisticated to keep pace.

*"It's a constant challenge of trying to be as prepared as you can be with an adversary who spends their day, all day, thinking about ways to infiltrate your system,"* says International SOS Senior Security Adviser Dave Komendat. His colleague, US Security Adviser Stevan Bernard, says reviewing widespread workforce access to apps which could spread vulnerability should be a priority.

Alongside these huge overlapping challenges, a range of underlying factors can compound risks and impair businesses' ability to respond. For instance, social divisions can be driven via social media, deepening prejudices and distrust. The febrile atmosphere this creates sees expression in attacks on politicians or corporate executives, and in workplace violence. Recent attacks in the West have increasingly involved lone individuals, but the broader threat of terrorism persists. At the same time, the falling cost of advanced drones makes remote attacks easier than ever.

11. United States CTIIC (2025) Worldwide Ransomware, 2024: Increasing Rate of Attacks Tempered by Law Enforcement Disruptions. Available at: https://www.dni.gov/files/CTIIC/documents/products/Worldwide_Ransomware_2024.pdf

# The signal and the noise

Businesses prefer to trade in **stable regulatory and political conditions** - even when those conditions aren't 100% favourable to them - rather than trying to ride unpredictable waves of change.

But the global political fractures that appeared in 2025, overlaying existing conflicts and tensions, removed any prospect of calm seas in the coming year. The speed of change in policy and political settlements leaves organisations operating in an ambiguous environment where all they can expect is the unexpected.

**Two-thirds of our Survey respondents**

**66%**

**say uncertainty has been an increasingly prominent feature of their risk landscape in the past 12 months.**

That's no surprise; 2025 was an inflexion point, as the assumption that stable global trading environments were in the interest of most nations was challenged. Globalisation has stalled, as businesses face rising barriers to trade, supply chains and talent, while governments increasingly prioritise national interests ahead of enabling global business.

The growth of tariffs, sanctions and supply chain disruptions, have made geopolitical uncertainties every organisation's concern. *"So domestic businesses need to start looking at that a little more than I think they have,"* advises International SOS Senior Security Adviser Kelly Johnstone. *"And if you're an international business, you need to be all over it."*

Many organisations agree; geopolitical instability was the most common factor driving risk managers' uncertainty in our Survey, cited by almost half (47%) of respondents.

# A world at odds

Geopolitical tensions have direct security implications. 2025 saw a significant **increase in armed conflict and violence** in many locations.

This is likely to continue in 2026 given the persistent geopolitical tensions in some of the most volatile regions, such as the Middle East, Sub-Saharan Africa and the former Soviet Union. The Global Peace Index compiled by the Institute for Economics and Peace recorded 159 state-based conflicts in 2025, more than any year since the 1940s[12]. The continuing war in Ukraine, the Israel/Gaza hostilities, civil war in Sudan, territorial skirmishes between Cambodia and Thailand and air strikes by NATO countries against the Houthis in Yemen all contributed to regional instability.

Drone incursions into the airspace of EU states make the risk of conflict on European soil more real. As governments in Europe focus more on security within the region and increase defence spending, this will impact how businesses see and manage risk in such traditionally low-risk markets.

International SOS Senior Security Adviser Franco Fantozzi warns that the obvious focal points for organisations' security concerns, such as Ukraine or the Middle East, can leave others overlooked. *"Social tensions caused by economic conditions in areas such as southern Africa or South America, even when there haven't been recent security incidents, make it important that risk assessments are comprehensive,"* he says.

This is evident in the growth of protest movements in countries including Madagascar, Nepal and Peru over the past year, which adds further zones of enhanced risk to business operations and travel planning. Finally, digital networks and AI increasingly function as risk amplifiers. The effect of disinformation in the form of unfounded claims or deep fakes fuels political polarisation and undermines trust in state institutions. This ultimately enables extremist political ideologies and conspiracy theories to thrive. This combines with increasing voter indifference in many populations to destabilise governments and increase unrest and political violence.

## So what?

Against this background, organisations need to become more proficient at understanding, anticipating and addressing geopolitical risk. Given its fluid nature, it may require a combination of anticipatory and forecasting methodologies and robust detection and response capabilities to allow for effective mitigation. Organisations and teams with a flexible approach to integrating strategic and tactical intelligence in their decision-making are likely to be more resilient to such risks, and ultimately more successful at protecting people, assets and business value in today's geopolitically volatile world.

Our Survey shows that concern over geopolitical risk has spread to sectors previously considered insulated, such as government services and education. But despite the destabilising effects of geopolitical uncertainty only just over half of the organisations in our Survey

**55%**

**factor political change into their risk management, far fewer than are concerned about reputation and trust (75%) or regulatory change (69%).**

This suggests businesses may be underestimating the effects of shifts that have rendered their scenario planning out of date. Such misjudgements could hinder effective crisis response. The flux in geopolitics makes it hard to pin down as a factor in CEM systems built to assess and mitigate known, definable risks. It is precisely that flux that makes organisations vulnerable to its impacts and is more reason for leaders to focus on it as a priority.

In the coming years, AI may help us sift huge volumes of data to better assess risk signals and produce instant, personally tailored briefs. In the near term, growing demand for energy and materials to support its development could increase geopolitical tensions and economic instability. Investors also worry that returns may lag spending, raising fears of a bubble.

## Risks factored into organisational risk management

- Risks which affect trust and reputation
- Risks from regulatory change
- Risks which affect how we live up to our values and standards
- Risks from political change
- Don't know

*"Uncertainty and instability in the region can't be predicted. The geopolitical landscape changes rapidly and impacts on our community directly and indirectly."*

**Security, Middle East**

12. Institute for Economics & Peace Global Peace Index 2025. Available at: https://www.visionofhumanity.org/wp-content/uploads/2025/06/Global-Peace-Index-2025-web.pdf


# The truth gap

We have been highlighting the **growing risk** of information overload and dis/misinformation for the past five years.

Unfortunately, we expect the problem to continue to accelerate through 2026, compounded by gaps in information. New regulations, guidelines and guardrails are being rapidly outdated. Only 14% of our Survey participants rated misinformation and disinformation as a source of uncertainty in their risk management but it seems likely they are underrating its disruptive potential.

The World Economic Forum has ranked misinformation among the top threats of the next decade. As misinformation spreads so rapidly, we are left navigating a global health crisis with a compass whose dial no longer points to the truth. Traditionally, public health and medical experts have relied on agreed evidence to make informed decisions for the populations they serve. While recommendations and policies vary, these processes are grounded in professional standards, guided by codes of conduct, peer review and mandatory disclosure of conflicts of interest.

Today, this landscape is shifting. Information is no longer confined to experts; anyone can share content, while oversight, accountability, rules and regulations are limited. Spotting AI-generated video becomes harder every day. The Doomsday Clock's Science and Security Board warns that the world is *"the closest it has ever been to catastrophe"*, in part due to "the spread of misinformation, disinformation, and conspiracy theories that degrade the communication ecosystem and increasingly blur the line between truth and falsehood" and a *"battered information landscape"*[14]. Add to this the increasing gaps in disease surveillance data identified by the World Health Organization following reduced funding for staff and health programmes, and discontinuation of trusted data sources for weather forecasting, the balance is tipped further toward misinformation and enlarging blind spots[14].

**One study estimates that about**

**50%**

**of the information on the internet has been machine-generated.**[13]

13. Graphite (2024) More articles are now created by AI than humans. Available at: https://graphite.io/five-percent/more-articles-are-now-created-by-ai-than-humans
14. World Economic Forum Global Risks Report 2025. Available at: https://www.weforum.org/publications/global-risks-report-2025/

# Corporate conscience

Companies have **increasingly faced situations** where corporate values, ethical standards, or compliance obligations collide with political shifts, policy changes, or public sentiment.

For example, organisations boycotting Russian gas because of the Ukraine conflict have found themselves more reliant on coal-generated power, risking breaches of their emissions targets and obligations. *"It was easier for businesses a few years ago when there was consensus on the 'right thing to do',"* notes International SOS Global Security Director Cvete Koneska. *"That consensus has now very much diluted, leaving companies unsure of where the moral compass lies."*

Our risk Survey finds that organisations are still guided more by the aim to maintain trust with employees and customers in making risk decisions, and not only implement but exceed regulatory requirements.

**They are also extending those higher standards to their contractors;**

**71%**

**of the organisations we surveyed say they carry out due diligence on suppliers' security, health and wellbeing standards and the same proportion say they won't hesitate to cut ties with suppliers whose standards are found to fall short.**

## So what?

In a time of high uncertainty, businesses need to review risk assumptions and scenario plans made before the geopolitical upheavals of the past year. They must ensure that their strategies are still based on valid assumptions about the altered world in which they operate. Robust plans will account for the setbacks in globalisation, new barriers to trade and investment and growing competition over scarce natural resources that can fuel conflict.

In an increasingly polarised political arena, domestically and globally, organisations need to plan carefully with increasingly ideological audiences and divergent regional regulatory and policy requirements in mind. For all of these, they need dependable sources of intelligence to provide them with insight and help reduce ambiguity.

Organisations must have robust processes to assess the quality of health information, with trusted sources and expert advisers to discuss complex issues, implications and, importantly, proportionate actions.

Strong intelligence is essential to separate the noise from the signals that matter to the organisation, and to design a method to anticipate, prioritise and respond to growing risks when the time is right.

## Hush trips – Where in the world?

The forced trial of home working triggered by pandemic movement restrictions at the start of the decade has persisted. Organisations recognised a large proportion of employees were keen to keep working away from their office base for some or all of the week. The sudden growth of location-independent working has thrown up a security and health concern in the form of hush trips. An increasing number of businesses have been caught off-guard by calls for assistance from workers facing security or health crises in locations the organisation did not expect them to be working in.

Only around one in five (22%) of respondents in our Business Resilience Trends Survey say their organisation has the capacity to monitor employee hush trips and only one in six (17%) say they are equipped to handle security or medical incidents that happen in these circumstances.

Whether they are visiting family or simply taking working vacations, individuals may feel it isn't important to inform their employer where they are as long as their productivity doesn't suffer, but in an emergency, many will still assume the organisation's Duty of Care follows them wherever they spend their working hours. How far employers' legal duties stretch in this grey area hasn't yet been tested in courts. However, every business needs to decide where it stands in advance of an alert from an unsuspected location from someone who needs immediate treatment, support or evacuation. It is also important to consider that employees on hush trips may also need support for accompanying travellers.

Hush trips must be accounted for in travel management procedures and crisis response procedures and checked for insurance coverage. Organisations need to decide what level of assistance they will to give to people who haven't disclosed their whereabouts. As a minimum, employee communications should strongly encourage checking with managers before relocating for any period and should make it clear that organisational support may not be as comprehensive in unflagged locations.

**Only 50%**
**of security and health experts in our Survey say their policies state the acceptable boundaries of remote working.**

### So what?

Hush trips represent a growing blind spot in Duty of Care, and most organisations are not yet equipped to manage the risks. As remote work remains a common request from employees, businesses must update their travel management and crisis response procedures to reflect this new reality. Clear policies, expectations and communication are essential to avoid gaps in support and ensure that employees understand the limits of assistance when working from undisclosed locations.

*"Companies need to do their very best wherever their employees are, but I think employees also have a responsibility to be honest and transparent with their employer about where they're conducting business, especially if it's different from where the company expects them to be."*

**Dave Komendat**
International SOS Senior Security Adviser

# Rising to the challenge

The evidence of our Business Risk Resilience Survey detailed in this report confirms how daunting a task many organisations feel they face in managing business risk.

Protecting their people and ensuring continuity is hard in a fractured world, where threats develop simultaneously and faster than ever and where information streams may be polluted by misinformation.

Security, health and business risk leaders, as well as the organisations they work for, have it within them to meet these challenges. Knowing the scale of the threats is part of the solution – forewarned is forearmed – and gathering the resources and external expertise to deal with them is another vital component. With the best intelligence and support, businesses will safely traverse the uncertain risk landscape of 2026 and beyond.

echo

INTERNATIONAL SOS

International SOS is in the business of saving lives and protecting your global workforce from health and security risks in a fragmenting world. We care for **+9,000 organisations**, from more than **1,200 locations** in **90 countries**. Partnering with International SOS can help you strengthen your organisation´s resilience, improve your employees' health and wellbeing, and ultimately, reduce your costs.

**WORLDWIDE REACH. HUMAN TOUCH.**

**internationalsos.com**