headspring
executive development

LEADING YOUR ORGANISATION THROUGH POLITICAL TURMOIL

A guide for senior decision makers to understand and respond to geopolitical risks | 2022

A joint venture of FT FINANCIAL TIMES | ie BUSINESS SCHOOL

headspring
executive development

ABOUT THIS REPORT

Leading your organisation through political turmoil was produced by Headspring Executive Development to help clients navigate through unprecedented levels of global uncertainty. Today's leaders must understand where threats come from, how likely they are to occur, what impact they will have on your company, and how to prepare and respond. Headspring offers a way forward.

Our analysis is based on the belief that every company is unique and requires customised solutions; that a company's internal challenges are as significant as the external threats; and that insights must be innovative, relevant and impactful.

The report was written by Alasdair Ross, an expert in geopolitical risk, and edited by Paul Lewis, Headspring's Editorial Director.

Contents

INTRODUCTION

The elements of political risk analysis

On 24th February 2022, Russia escalated its conflict in Ukraine by launching a major military attack. Moscow's intention was to overthrow Ukraine's western leaning government and assert control over its eastern regions. Western governments were outraged. The US, EU and others imposed heavy sanctions, with the aim of crippling Russia's economy. As a result, some of the world's biggest brands, including McDonalds, Coca Cola, and BP – icons of the post-Soviet transition – jettisoned more than three decades of investment, and withdrew from the market. Write-downs ran into the billions of dollars. Corporate reputations, nurtured painstakingly over decades, were shredded within days.

But what, perhaps, was most striking was that the pressure to withdraw came not so much from the new tougher operating environment in the host market – these companies had weathered fiercer storms – but from home country governments and their increasingly socially aware and activist consumers. For companies that believed they had mastered geopolitical risk, this was a loud wake-up call that few if any had anticipated.

No matter how tightly a company controls its own operations or minimises risk in its personnel and procedures, threats can emerge from places beyond the company's control. These external risks can be difficult to spot and harder to remedy.

Companies can start by distinguishing between events that can be anticipated and mitigated—such as labour conflicts or regulatory change—and unexpected developments, such as coups d'état, bank runs or surprise devaluations. Although some investors seem content to do nothing and hope for the best, a systematic and carefully planned approach allows companies to anticipate many risks, understand their relative importance to the company and then plan appropriate remedial action.

'MANAGING RISK NOT ONLY REQUIRES COMPANIES TO IDENTIFY A THREAT, BUT ALSO UNDERSTAND HOW IT INTERSECTS WITH THEIR INTERESTS.'

Unfortunately, effective risk management is complex, because every company views risks differently. Even close competitors operating in similar product markets have their own unique dynamics. So managing risk not only requires companies to identify a threat, but also understand how it intersects with their interests.

INTRODUCTION | The elements of political risk analysis

However, a simple framework based on the five actions can help executives react effectively:

- **Scan the horizon**
  What is the range of risk events out there, and their probability of occurring? General Motors, the US carmaker, has some 400 major partners in its supply chain, manufacturing plants in 20 countries from Argentina to Vietnam, and consumers in just about every market in the world. Disruption in any of these locations could affect operations much further afield, denting sales and profits. Companies similarly exposed across multiple markets need teams to gather and interpret intelligence on developments that may affect operations, whether to do with local politics, security, laws and regulations or the myriad other vagaries of the external environment that are affected by political dynamics.

- **Calculate exposure**
  For each risk, how much does the company have at stake. Even where the likelihood and timing of a risk event is clear, every companies' exposure will differ. For General Motors, a failure at Lear Corporation, with which it spends around $250bn a year on seats and other equipment, would be costlier than one at Remy International, a maker of alternators and other electronic equipment, with which it spends a tenth of that amount. A company might be exposed, for example, through falling revenues, lost production days, supply chain disruption, reputation damage.

- **Determine your risk appetite**
  How much risk is the company willing to take? This depends on several factors. Well-funded start-ups in fast-growing industries may be hungry for risk; established corporations operating on narrow margins in heavily regulated industries, less so. Ultimately, the willingness to accept a certain level of risk depends on the trade-off between potential cost and reward. If such a cost-benefit calculation can be expressed in dollar terms, it can be made quite precise, though many CEOs prefer a 'seat of the pants' test to what might be viewed as a spurious formula.

- **Assess your resilience**
  How prepared is the company to confront the risk? What mechanisms/skills/hedges are already in place to mitigate potential damage? Resilience is largely a function of how well a company has performed the above three steps, and its readiness to respond. Building resilience—a company's protective armour—is the purpose of risk management. Resilience is developed by making well-informed, timely decisions about where and how to set up operations, and deploying people and resources to address threats and exploit opportunities as they arise. For example, Royal Dutch Shell protects itself from potential protesters disrupting exploration by consulting with Greenpeace.

- **Respond**
  Broadly speaking, there are three meaningful responses to a threat. First, accept it. If it's unlikely to occur and its impact on your business likely to be modest, one might simply say 'bring it on' and deal with the consequences when they arise. Second, transfer the risk. A broad range of complex insurance and hedging instruments are available allowing you to shift the risk to specialist companies. Third, increase your preparedness and resilience—hiring additional expertise or investing in otherwise redundant systems might make the risk more tolerable and allows you to stay in the market. And it is this third option where managers must draw up their own, company-specific, taxonomy of scenarios, vulnerabilities and actions that will guide leaders how to act when a crisis hits.

PART 1

Where and how to look for risks

Key takeaways

Governance, regulation and infrastructure are key areas where risks arise

Determine who is responsible – a CRO, key departments or others

Use 'bottom-up' and 'top-down' techniques to capture unexpected and strategic threats

Recent geopolitical events have thrown up renewed scope for business disruption. War, civil unrest or a sudden change of government can destroy demand for a company's products, besmirch its reputation in the host or home market, disrupt logistics lifelines, and threaten the safety of staff. A single event can cascade through the organisation and manifest in different ways over time. Its impact can be direct or indirect, or dormant until it combines with other risks to produce further, unintended and unexpected consequences.

Furthermore, a geopolitical crisis can be capricious. It can devastate one market, while leaving a neighbouring market unscathed. Even within the same market, an event may be perceived differently, depending on a company's business model, sector, value chain or processes.

There is no single accepted taxonomy of political risk that companies (outside the financial sector) can adopt. This makes it particularly hard to identify the source of a threat, let alone calculate its impact on your company. But that shouldn't deter companies from trying. As risk managers rightly warn: the costliest risk is often the one you hadn't thought of.

Nevertheless, a systematic assessment might begin by exploring the following categories of political risk that your company may face:

Governance

Investors depend on high-quality, stable government that can get things done. It helps if the administration's policies are generally pro-business and responsive to investors' concerns. But a ruling party's stated policy aims—and its commitment to them—can easily change. Governments often struggle to implement policies because of weak coalitions or unreliable parliamentary majorities. An election might be looming with an opposition that wants radical change. There may be fierce resistance to reform, for example from trade unions, organised crime, or other embedded vested interests. Even in the best circumstances, transitions between one administration and the next can prolong uncertainty.

PART 1 | Where and how to look for risks

Ford Motor Company is among dozens of corporations that became the target of unexpected—and unwelcome—attention following Donald Trump's 2016 US presidential election. Before even taking office he launched a Twitter attack citing Ford plans to move production of its Lincoln model from Kentucky to Mexico. The US was 'getting killed,' he protested. When Ford announced that it would not transfer production (indeed, had never planned to) the company dodged a political bullet. But the incident made clear that there were new 'rules of the game'.

Regulation and public policy

All companies operate within a dense network of laws and regulations that set competition rules and protect citizens and consumers. Rules tend to be tougher in sectors such as finance, pharma and airlines where the danger to the public is potentially greater. However, the system may be 'captured' by vested interests. In some emerging markets, investors may believe that it's easier to breach the rules and pay the fine than to seek official permission. But the consequences are not always limited to a fine.

German carmaker Volkswagen discovered this in 2015 when it was found to have cheated emissions tests. The company has since provisioned around $30bn against prospective fines and the cost of vehicle recalls and replacements, to say nothing of its reputation. Indeed, the scandal has harmed Germany's automotive industry more generally.

QUESTIONS TO ASK

- Is the government willing and able to create or maintain an attractive business environment?
- Is a future administration likely to change the rules retrospectively or without warning?
- Do government transitions follow clear and uncontested rules?

QUESTIONS TO ASK

- Who is acting against our commercial interests, how and why?
- Who are the key influencers of public policy, and can we speak to them?
- What are the real costs of non-compliance?

PART 1 | Where and how to look for risks

Security

Some markets are particularly prone to theft, terrorism or violent crime. An unlucky company might find itself a direct target of protest as authorities appear powerless or unwilling to act. It may be because a brand has political or national symbolism. In 2012, Chinese protestors, enraged over Japanese actions in the Senkaku islands (known as Diaoyu in China) over which both countries claim sovereignty, vandalised Japanese business assets across a swathe of provinces while the authorities stood by. Japanese-branded vehicles were torched where they stood. Honda, Toyota, Nissan and Mazda suspended production in plants around the country, as did Panasonic, Canon and Kobe Steel. In the auto industry alone, losses from suspended production reached $250m. Japanese goods exports to China slumped, as did China tourist arrivals in Japan.

A similar case arose with Southern Copper Corporation, a Mexican mining company, which had planned to break ground on its Tia Maria copper mining project in Peru in 2011. But the venture ran afoul of local farming communities who said it threatened their livelihoods. Six protestors died in clashes with police, and the project is still awaiting government permission. As well as a local cause celebre, Tia Maria has become a political football for successive national governments and a victim of Peru's endemic political instability.

QUESTIONS TO ASK

- Are we vulnerable to discrimination through national association?
- If we are subject to protests and disruption will the courts defend us?
- Can we do more to win public support for our projects?

Infrastructure, logistics and supply chains

Political risks may not threaten a company directly, but can disrupt points along its value chain, especially those that rely on 'just-in-time' delivery. It is not just terrorist attacks such as 9/11 that companies need to worry about. Ports, roads, railways, airfreight, broadband, cloud-based services and computer processing capacity can all be affected by militants, street protests, mass migration, or a simple lack of public investment.

PART 1 | Where and how to look for risks

Tata Motors and its suppliers faced such disruption in Kolkata, India when local farmers, forcibly displaced to make way, took to the streets. Backed by a high-profile media campaign, they eventually forced Tata to dismantle the plant, and rebuild it in Gujarat at great costs.

Neither this list nor any other can be exhaustive, and political actions and decisions can affect businesses in almost limitless ways. But by viewing the political risk landscape systematically and asking the right questions companies can minimise the likelihood that they will confront a threat they have not considered. Knowing where to look for risk is only part of the task. They also need to know what techniques they can use to identify risks and who is best placed to perform this task.

'THE COSTLIEST RISK IS OFTEN THE ONE YOU HADN'T THOUGHT OF.'

Odysseus lost six sailors and risked his life when he tried to navigate between Scylla and Charybdis. What Homer neglects to mention, however, is that our ancient hero lacked a system for gathering data on the two hazards and calculating a risk-reducing path between them.

QUESTIONS TO ASK

- Is there a history of civil unrest and government responses to consider?
- Are fiscal constraints likely to lead to deterioration in the quality of infrastructure?
- If a supplier fails, how quickly can we identify and secure a replacement?

Companies' first task is to decide who should be responsible for spotting risks. Much depends on the organisation's size and culture, though similar sized companies in similar sectors disagree on the matter. Some firms have a dedicated risk function and a Chief Risk Officer on the management committee. Others split responsibility between departments, with Finance, Legal, Compliance and Operations usually playing a role. The second task is to determine what techniques to use. Odysseus relied on eyes and ears. But generally, the more techniques used, the more comprehensive, diverse and reliable the resulting data will be (see box on page 10).

PART 1 | Where and how to look for risks

Different techniques will suit different companies in different circumstances. But companies should at least combine bottom-up and top-down systems. The former rely on those individuals who are closest to threats to identify and report them. The latter require those with strategic responsibility to view the full range of risks, spot how these might flow from one business area into another, and see which threats have strategic significance.

Some of the techniques companies use—either alone or with specialist support—are listed below:

YOUR PEOPLE AND PARTNERS

- **Analysing past mistakes.**
  Companies often start by looking to their own—or competitors'—histories for signs of what can go wrong. Institutional memory is crucial, so engage your long-serving staff members.
- **Staff and stakeholders.**
  Regional staff, suppliers and partners will have a distinct sense of local conditions and can pass these impressions up the chain informally or preferably through a systematic reporting process. A good example of a 'bottom-up' approach, it requires companies to foster a risk-awareness culture throughout the organisation, and create procedures that allow all employees to submit concerns. Remember, a shop floor worker in a remote manufacturing facility may perceive local threats more quickly than senior managers at HQ.
- **Service providers.**
  A company's banks, external legal team and other services partners usually provide valuable market intelligence, albeit designed to sell their services.
- **Buying specialist information.**
  Independent third-party analysis on politics and business conditions in key markets can supplement and test the company's own contacts on the ground, who may lack a macro perspective. This 'top-down' kind of intelligence will be generic, and you will still need to judge which risks are relevant to you and how they will affect your organisation.

PROCESSES

- **Brainstorming.**
  Free-wheeling discussions with senior cross-functional teams can throw up risks that none might have considered alone.
- **Strategic analysis.**
  A company's strategy process can be mined for risk implications. Explore the 'Threat' element of any SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis. A PEST (Politics, Economics, Social, Technology) analysis may also throw up risk management issues.
- **Project management.**
  Most include a section on risks to the project. The tendency is to focus on single issues relevant only to that project, but this is an opportunity to capture broader threats that might spill over into this project. It is also worth considering how failing to execute the project would affect the rest of the business, and to make sure that this risk is captured outside the project itself.
- **Regulatory requirements.**
  Some companies or departments, such as IT, may engage in formal risk reporting to meet regulatory requirements, which should then be incorporated into the broader corporate risk framework.

MODELS

- **Scenario planning.**
  Specialised external facilitators can help surface interconnected risks and plot their path through the company, and for 'war-gaming' the response. Methods run from loose narratives to complex statistical modelling, and it is important to identify a technique that is both relevant and practical.
- **The Delphi method.**
  A cross-functional panel responds independently to a questionnaire, and a facilitator consolidates the responses and issues subsequent rounds of questions, helps to avoid 'group think' and shares responsibility evenly.
- **Fault Tree Analysis.**
  FTA turns the risk identification process on its head by asking 'what do we really want NOT to happen?' and then investigating what would make it likely to occur. You DON'T want to be held up for bribing foreign officials, so asking what might lead staff or partners down such a path illuminates where the risk lies.
- **Root Cause Analysis.**
  This considers the deeper variables that underlie a headline threat. For instance, you might already understand how a transport workers strike would disrupt transit links to your factory. But thinking more deeply about the state of industrial relations ahead of a round of pay negotiations might provide an even earlier warning (not to mention help you forecast wage inflation).
- **The Bowtie method.**
  This examines how a single risk event might manifest across the organisation, usually resulting in a bow-tie shaped diagram. As well as a visual summary, it provides a systematic account of the contingent threats, and how failing to address the risk in one area could wend its way into others. The risk event sits in the middle; its possible causes and preventive actions sit on the left side; the consequences and post-hoc responses are on the right.

PART 2

How risks affect your business

Key takeaways

- A political event isn't a risk unless it affects your business
- Map out company-specific 'pathways of impact' from any crisis
- Simple measures, speedily implemented can mitigate potentially huge risks
- Determine beforehand which risks are worth mitigating to stay in your market

A favourite tactic of Shining Path guerrillas during Peru's insurgent war was to topple electricity pylons on the outskirts of the capital, plunging shops, streets, houses, factories and offices into darkness. Businesses faced disaster. Yet some companies, with contingency plans for a sudden, prolonged power cut, survived and prospered. What mattered was not just their foresight but the way they assessed the risks to their operations.

To make an effective calculation of political risk, companies must understand four key variables: the likelihood of the risk event happening; the degree to which they are exposed; their level of resilience, and the amount of risk they are willing to accept.

1. Probability

How likely is a particular risk event to happen? Peru's insurgency dragged on for years and disruption to the power supply was on everybody's radar, so few should have been taken by surprise. Blackouts were a high-probability event. Just over the border in Chile peace reigned and blackouts were very rare.

Judging probability is a vital calculation because a company's resources are scarce. One might anticipate any given external political event, but it can't be classified as a risk to the business unless it can also affect business operations—otherwise, it is just a headline to be read and forgotten.

If we could predict future events with precision there would be no such thing as risk, so how do we assess probability? The past—a record of the event's frequency over time—can be a guide, though the past is a notoriously unreliable predictor of the future. The most straightforward assessment technique is to rank events in order of their perceived likelihood. If you can't say how likely event A is, you may be able to judge whether it is more or less likely than event B. Such a ranking can provide sufficient data for an effective risk model.

This qualitative approach is often required with political risk. Given the range and uncertainty of political variables, the kinds of quantitative techniques used in finance can be dangerously spurious.

2. Degree of exposure

How exposed is your company to the particular threat? The way an event affects business will vary from company to company, and will depend on what we can call the 'pathway of impact'.

During Lima's blackouts, primary healthcare providers faced disruption to surgery schedules and potential lawsuits over the effects of delayed medical attention. In the same circumstances steel company Siderperu faced disaster if blast furnaces cooled with semi-processed material in the production line. The computer systems and ATM networks of the country's banks were exposed to power surges as the distribution network came back on line, with the potential for data loss, hardware damage and client disaffection.

In each case, the same event had different effects and worked its way through the organisation in different ways, with a cascade of primary and secondary impacts as the organisation responded.

Companies must also ask how important the disrupted part of the business is in the whole organisation. For Siderperu, whose entire operation was based in Peru, the consequences could have been catastrophic. For those commercial banks that were subsidiaries of major multinational institutions the impact on the wider group was more manageable.

Measuring exposure to political risk is an art rather than a science. Financial risk can be expressed in terms of the expected impact on revenue, but politics is less tangible and transparent. Again, a ranking system agreed in discussion with relevant department heads can provide the basis for calculation.

'JUDGING RESILIENCE IS NOT ONLY A MATTER OF HOW A COMPANY RESPONDS, BUT HOW FAST.'

3. Resilience

How protected is the company from the identified threat? Peru's banks, along with many other local companies, had installed emergency generators that kicked in when the electricity grid failed (assuming diesel supplies held out), and batteries to keep the lights on while the generators started up. These mitigations made them resilient in the face of power disruptions.

Private clinics used flexible staffing rotas to bolster coverage when disruption prevented staff from getting to work. Public hospitals, victims of a crisis in public funding at the time, were unable to copy them and, as patients discovered to their cost, were less resilient.

For other companies, a simple system that enabled staff to work at home could mitigate the worst of the disruption; resilience need not be expensive.

Judging resilience is not only a matter of how a company responds, but how fast, which boils down to the following:

Decisive action – have responses to threats been identified, and are mitigation plans ready to be activated at short notice?

Clear responsibility – have the right people been given the responsibility and the skills to implement the plan, as well as the autonomy to adapt when circumstances change?

Practised procedures – does the company practise for crises in a realistic way, as one might in a fire drill? Mere box-ticking exercises are more likely to breed complacency than resilience.

4. Risk appetite

There will always be some risk in any business venture. The key question is how much risk a company can handle for a given reward. Sometimes, it's the CEO who decides (given that it's his or her head on the block). Companies with more sophisticated risk management processes can produce a formal risk appetite statement to cover every major risk identified. This statement recognises the relative importance of the company's strategic and operational objectives, and the degree of risk the company would be willing to take to achieve each of them. For instance, a company might be willing to take more risk for an acquisition that opens a large new client base than for one that builds scale in small existing markets.

Companies, and even entire sectors, can be infused with a culture of risk (or risk avoidance). Silicon Valley start-ups are notoriously uncertain ventures and require a voracious appetite for risk. The private banking houses of London and Geneva are protective of their history and will set a high price for the risks they accept. For Siderperu, the quality and reliability of supply was the company's most valuable asset, and therefore the area where there was least appetite for risk taking. For the private clinics, it was reputation.

The risk calculation

The above four variables —probability, exposure, resilience and appetite—have a critical part to play in planning a response to risk. Even highly unlikely events can push a company with high exposure and low resilience beyond its tolerance.

Once the risk horizon has been mapped, these four variables should determine the priority the company gives to each risk, and therefore the share of its resources it deploys against them. It will also form the basis of a simple framework for each company to categorise and prioritise the risks they face, and design appropriate responses.

headspring
executive development

PART 3

A practical framework for action

Key takeaways

- Political risks can be quantified and represented within a single matrix
- Threats to the business must be mapped against its willingness and ability to absorb risks
- An effective risk matrix helps senior managers reallocate resources
- Executives at national or functional level can identify their own risk and response picture

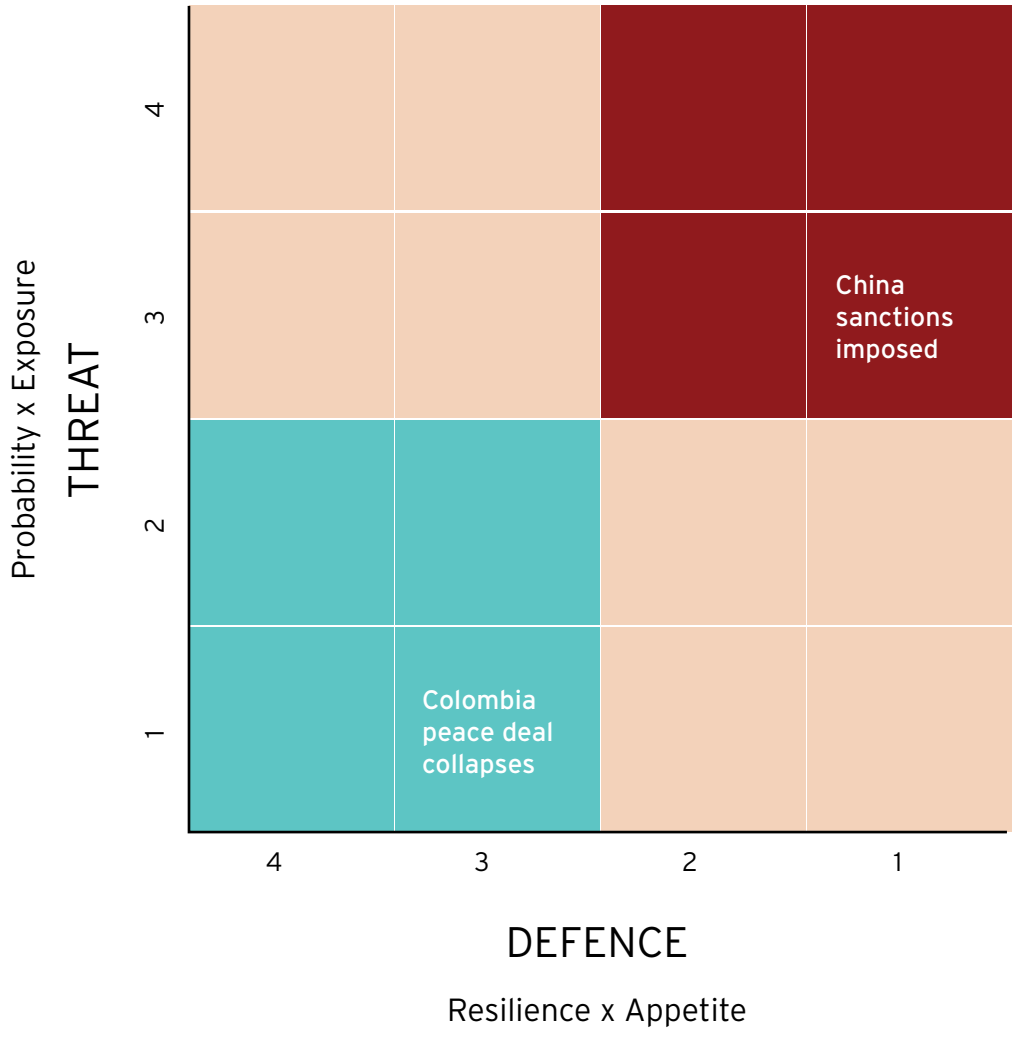
Earlier, we introduced the elements needed to identify, quantify and prioritise the risks that a company faces; assess a company's appetite for a given risk in a given circumstance; and help executives throughout the company to prepare for the worst.

Drawing these variables into a simple framework provides decision makers with an overall view of where the company's geopolitical risks lie thereby helping them allocate resources, assign responsibilities, and ultimately seize good business opportunities. An effective framework can also encourage collaboration between departments that face related risks and require a coordinated response.

Importantly, a risk framework must be tailored to the priorities and structure of each company. The first step to achieve this is to separate the variables that represent the threat level to the business from those that show its capacity or willingness to absorb it. In the former, we count the probability of the risk event occurring and the company's exposure to it. The threat level is a simple product of these two measures. For defence, we combine the company's resilience and its appetite for risk. Both calculations can be represented as an indicator on a scale of one to four, though individual companies can refine the scale of measurement if necessary.

Matrix reloaded

Risks can then be plotted in a matrix, colour coded to show at a glance the priorities (see chart below). So a risk with a low threat score and a high defence score would sit in the green quadrant, indicating low priority. But a high threat with a low defence score would sit in the red, high-priority quadrant. Risks with either high threat level and high defence level, or low threat level and low defence level, would sit in orange moderate-priority quadrants.



Source: *Headspring Executive Development*

PART 3 | A practical framework for action

Consider some real-world examples. A Brazilian drinks manufacturer with markets around Latin America might classify the prospect of a collapse in the peace deal between Colombia's government and FARC insurgency as a risk. The peace deal looks sound, so the probability of this happening is low, and the company might judge its Colombia exposure to be modest in any case. This would equate to a low threat score. At the same time, since the peace deal is recent, the company's Colombia operations may already be optimised for an insecure situation, so resilience is high. Maintaining a physical presence in the country may be an important element in the company's appeal to the local market, so it may be willing to accept a higher level of risk (its risk appetite) than otherwise. With both strong resilience and appetite, the defence score for this risk is high. These scores—low threat and high defence—would place the risk firmly in the green quadrant, and resources would be prioritised accordingly. For example, it may be that it that any risk can be dealt with at local level.

'A HIGH THREAT WITH A LOW DEFENCE SCORE WOULD SIT IN THE RED, HIGH-PRIORITY QUADRANT; COMPANIES WILL NEED BACK-UP PLANS AND PROBABLY SENIOR LEADERSHIP INVOLVEMENT.'

Meanwhile, a US consumer goods manufacturer might view China's market quite differently given the prospects of higher tariffs in the wake of the country's worsening relations with the Trump administration. If the company already has a major operation in China this implies a high risk exposure, especially if leaving the market would damage its global growth. If the company also finds that its local connections turn out not to be as reliable as previously thought, the company may have little resilience against business disruption there. At the same time, if the company's name and reputation in markets elsewhere are on the line, it may have little appetite for dealing with new problems in China. With a high threat score and a low defence score, this risk would sit in the high-priority red quadrant of the company's risk register. Companies will need back-up plans if things go wrong, and the global leadership may need to be involved.

PART 3 | A practical framework for action

The matrix can be repeated at departmental level too, where the variables may differ from the general company level. For instance, a local subsidiary may see a mix of threats to its operations from a transport strike against public sector reforms. For operations and procurement, the threat may be severe; for finance and marketing it may be modest. Separate risk matrices for each of these departments will reflect the degree of threat they face and help to determine how much attention should be paid to the underlying risk.

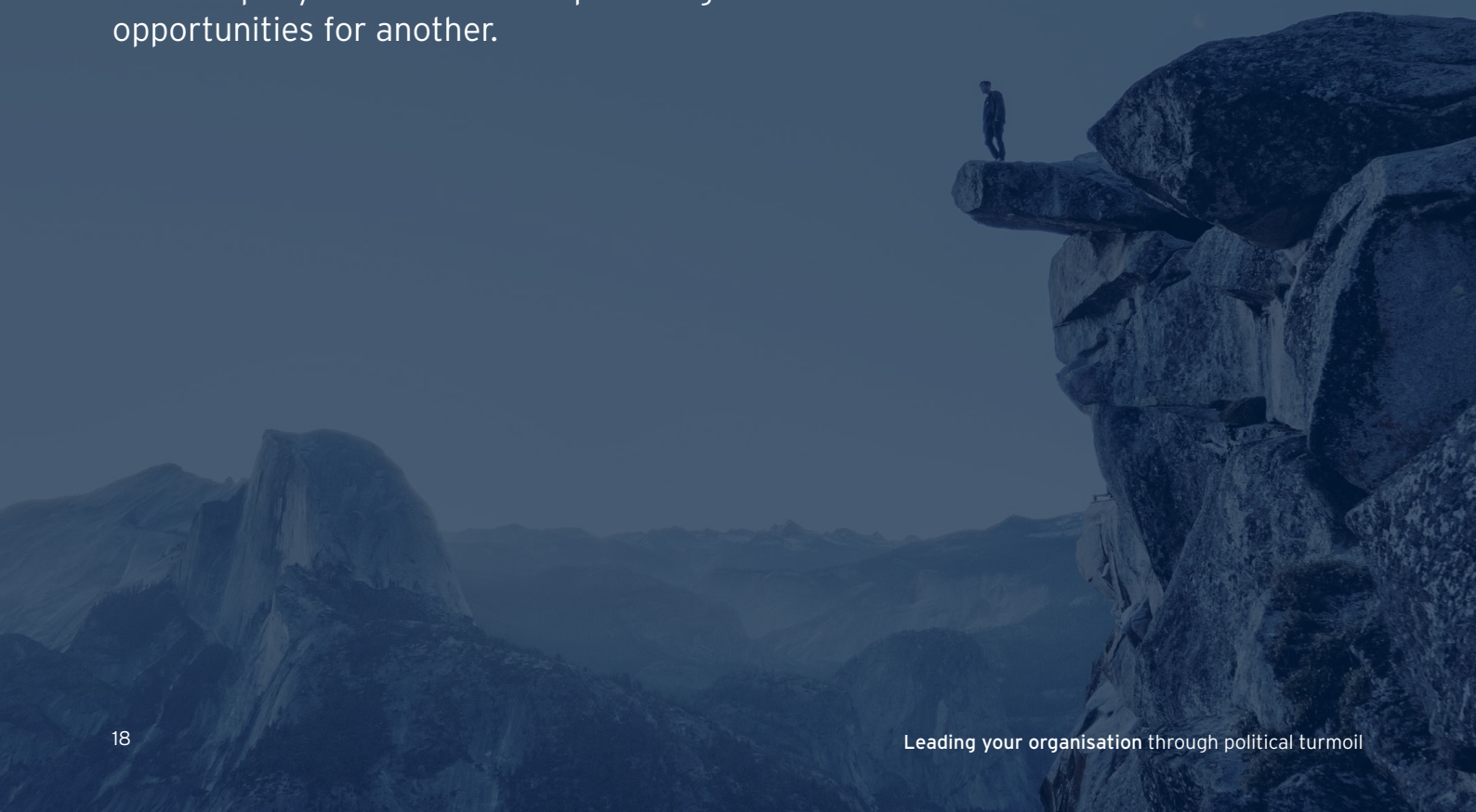
Each company will go through its full register of political risks, assign them threat and defence scores, and locate them on the matrix. Fully populated and regularly updated – as new threats emerge and departments enhance their resilience or reduce exposure – the matrix provides senior management with an instant, up-to-date view of the number and intensity of major geopolitical risks worldwide. A bias towards amber and green may free up resources for other uses. A preponderance of risks in the red quadrant will alert the management to the need for more resources and action should the worst happen.

CONCLUSION

Executives face a bewildering array of geopolitical threats. Some high-risk events can be identified from a cursory reading of the newspapers. Well-informed leaders may also be able to assess the likelihood of such risks occurring. Other situations demand more in-depth analysis. Either way, an awareness of international events is only the first step towards protecting your business. Why? Because every company sees risk through its own unique lens. The potential for harm will depend on the sector in which a company operates, its strategy and geographic reach, its operational exposure, and much more. A single event might spell trouble for one company or division while providing opportunities for another.

Equally important will be the resources and experience that a company can draw upon in the face of political crisis. Moreover, some company cultures may feel more at home in politically risky markets; others might seek to protect their reputation at all costs. In short, every company must decide its own particular risk profile and its own response to each identified threat.

This analysis shows senior executives how to start thinking about political risks. It clarifies the complex interplay of factors that can endanger your company. And it gives decision makers the confidence to map out a plan of action should danger strike.




headspring
executive development
headspringexecutive.com
A joint venture of:
FT
FINANCIAL TIMES
ie
BUSINESS SCHOOL