5º

BOOK CLUB SYNOPSIS

Political Risk: How Businesses and Organizations Can Anticipate Global Insecurity
Condoleezza Rice and Amy B. Zegart

Twelve, 2018

CONTENTS

01

CHAPTER ONE

THE *BLACKFISH* EFFECT: TWENTY-FIRST-CENTURY POLITICAL RISK

Just 18 months after completing a successful IPO that raised more than $700 million in capital and produced a valuation of $2.5 billion, "SeaWorld Entertainment's fairy tale had become a nightmare." The stock price fell 60 percent, and CEO Jim Atchison resigned. What happened? Filmmaker Gabriela Cowperthwaite released an investigative documentary called *Blackfish*, which argued that SeaWorld's treatment of orcas endangered both humans and whales. It was quickly endorsed by celebrities and animal rights activists, and corporate partners began cutting ties with SeaWorld. Even federal regulators and state legislators got involved. At the end, SeaWorld's business had been perhaps irreparably damaged.

Authors Condoleezza Rice and Amy B. Zegart attribute the film's impact thusly: "Atchison and SeaWorld were blindsided by political risk. Not just any kind of political risk, but twenty-first-century political risk, where the political actions of small groups, or even lone individuals, supercharged by connective technologies, can dramatically impact businesses of all kinds."

Political actions need not involve a government or political party. The internet and global connectivity have enabled nonstate actors to exert pressures with sometimes far-reaching effects. "Increasingly, political actions that impact businesses are happening everywhere."

In constructing the course that this book is based on, Rice and Zegart surveyed the literature exploring political risk's impact on global business and found it lacking. They began to collect their own case studies and develop the simulations contained in this book. "Our goal ... is to offer a useful framework that can be deployed in any company to improve political risk management. Our bottom line is your bottom line: Companies that best anticipate and manage political risk will have the strongest competitive edge." Their framework has four stages: understand, analyze, mitigate and respond.

GUIDING QUESTIONS FOR EFFECTIVE RISK MANAGEMENT

Understand

1. What is my organization's political risk appetite?
2. Is there a shared understanding of our risk appetite? If not, how can we foster one?
3. How can we reduce blind spots?

Analyze

1. How can we get good information about the political risks we face?
2. How can we ensure rigorous analysis?
3. How can we integrate political risk analysis into business decisions?

Mitigate

1. How can we reduce exposure to the risks we have identified?
2. Do we have a good system in place for timely warning and action?
3. How can we limit the damage when something bad happens?

Respond

1. Are we capitalizing on near misses?
2. Are we reacting effectively to crises?
3. Are we developing mechanisms for continuous learning?

02

CHAPTER TWO

MOVE OVER, HUGO CHÁVEZ

In nationalizing his country's economy, Venezuelan President Hugo Chávez seized, among other things, 11 oil rigs from U.S.-based Helmerich & Payne, a rice mill from Cargill, and the local operations of Mexican cement company Cemex. But this kind of risk is no longer the norm. Instead, a variety of actors interact with one another in a complicated web. Rice and Zegart group them into five major "levels of action."

Individuals | "Twitter users, documentary filmmakers, activists, consumer advocates, celebrities, ordinary citizens, and bystanders"

Local organizations | "neighborhood associations, political groups, and local governments"

National governmental actors and their institutions | "presidents, executive agencies, legislatures, and the judiciary"

Transnational groups | "activists, terrorists, hackers, criminals, militias, and ethnic or religious communities"

Supranational and international institutions | "the European Union and the United Nations"

INDIVIDUALS

"Changing a company policy no longer requires face-to-face organizing, around-the-clock picketing, or testimony before Congress. Connective technologies enable people to organize and their messages to 'go viral.'" United Airlines learned this lesson the hard way, after footage of Dr. David Dao being beaten up and dragged off one of its planes triggered worldwide criticism and led to more than $255 million in lost shareholder value.

LOCAL ORGANIZATIONS

In 2015, although the U.N. Security Council's permanent members and Germany agreed to lift U.N. sanctions on Iran, the economic growth promised failed to materialize. Why? Because 32 American states had their own laws restricting investment in Iran, and there was little that could be done in the face of governors unwilling to bow to the federal government on the matter.

Another example: In 2014, a longshoreman labor dispute led to months of port congestion in Los Angeles and Long Beach. While large companies were able to reroute their shipments, many smaller shippers could not. "The Agriculture Transportation Coalition estimated that losses in agricultural sales reached $1.75 billion per month" over the nine-month strike.

NIMBY ("not in my backyard") movements pose similar issues; the Keystone XL pipeline was first challenged by local ranchers, then the opposition gained national momentum, and President Obama halted its construction. "Companies that manage risks well recognize the importance of building relationships with local stakeholders before opposition mounts." In other words, "Being a good neighbor is good business."

NATIONAL GOVERNMENTAL ACTORS AND THEIR INSTITUTIONS

"National governments pose evident risks through their power to tax, regulate, confiscate, expropriate, make or break commitments, and shape capital markets." Regardless of governmental structure, all governments are organized in ways that create competition over influence and resources. And jurisdictional lines of authority can often be unclear or require careful negotiating. After the fall of the USSR, for example, companies like Chevron were left to figure out whether contracts formed with the USSR were still valid in newly independent countries.

"More often, national governments as a whole pose risks. Most countries consider particular industries to be intimately tied to the national interest. These are called 'strategic industries.'" For example, Russia has used its state-owned energy giant Gazprom to cut off supplies to Europe at politically opportune times. Although some countries, like the U.S., are very resistant to the idea of state-owned industries or enterprises, "most countries consider some key industries to be within the national interest and will use the full power of the state to protect them. Companies seeking to move into a foreign market would be wise to understand whether their industry is one of them and plan accordingly."

TRANSNATIONAL GROUPS

"Technology has enabled transnational groups of all types … to become more significant sources of risk for businesses." This has led to the rise of cybercriminals, including those who are merely in it for the money and "hacktivists" such as Anonymous or LulzSec, whose malicious internet escapades are fueled by ideology. In June 2017, a cyberattack called "NotPetya" spread across the globe, holding hard drives around the world ransom and damaging them in the process. Russian oil company Rosneft and American pharmaceutical company Merck were among those affected, demonstrating the ease with which criminals can target resources globally.

SUPRANATIONAL AND INTERNATIONAL INSTITUTIONS

"If individuals lie at one end of the 'level of action' spectrum, supranational and international institutions lie at the other." These "formalized organizations that bind countries and hundreds of millions of people together … can impose their will deep inside the economies and societies of member states." The EU and U.N. are such institutions. But, along with the bureaucracy comes the same issues that often keep other governmental organizations from making a big difference: questions of enforcement, ultimate accountability and simple disagreement.

TEN TYPES OF POLITICAL RISK

1. **Geopolitics |** Interstate wars, great power shifts, multilateral economic sanctions and interventions
2. **Internal conflict |** Social unrest, ethnic violence, migration, nationalism, separatism, federalism, civil wars, coups, revolutions
3. **Laws, regulations, policies |** Changes in foreign ownership rules, taxation, environmental regulations, national laws
4. **Breaches of contract |** Government reneging on contracts, including expropriations and politically motivated credit defaults
5. **Corruption |** Discriminatory taxation, systemic bribery
6. **Extraterritorial reach |** Unilateral sanctions, criminal investigations and prosecutions
7. **Natural resource manipulation |** Politically motivated changes in supply of energy, rare earth minerals
8. **Social activism |** Events or opinions that "go viral," facilitating collective action
9. **Terrorism |** Politically motivated threats or use of violence against persons, property
10. **Cyber threats |** Theft or destruction of intellectual property, espionage, extortion, massive disruption of companies, industries, governments, societies

GEOPOLITICAL EVENTS

"First and most broadly, political risks arise from geopolitical events like major wars, great power shifts, and the imposition of multilateral sanctions or military interventions." While the direct effects of such events are plain, indirect effects can be equally important to consider. In 2003, shortly before the U.S. invasion of Iraq, Dow Corning "decided to stockpile inventory and accelerate its own shipping schedule" in response to an anticipated decrease in shipping capacity. This decision prevented an interruption in its business when the armed conflict began.

INTERNAL CONFLICT

"Internal conflicts include social unrest, ethnic violence, and federalist discord about the appropriate allocation of power between central and regional governments." These may eventually lead to civil wars, coups and revolutions, which in turn can produce mass migration of refugees. In 2015, more than 65 million people (one in 113) were displaced due to political unrest or persecution. Coups have been found to reduce national income by 7 percent, and economic growth slows by 2.1 percent in the year of a coup. The risks for even the most prepared and best-intentioned companies are clear.

LAWS, REGULATIONS, AND POLICIES

"Businesses can miss and get burned by legal, regulatory, or policy changes if they assume that political stability and policy stability are the same thing." In 2011, Irish energy company San Leon Energy was interested in beginning a shale gas fracking industry in Poland. But before anything had been done, the Polish government proposed an 80 percent tax rate and heavy state ownership of any such energy project. The industry was essentially dead on arrival.

Rice and Zegart recommend thinking about policies, laws and regulations along a continuum. "At one end of that continuum are those that are almost always changing in some way, like taxes, and that typically result in incremental, manageable effects for global businesses.

… In the middle of the continuum are policies like foreign ownership rules that change less frequently but when they do change are typically more consequential. At the extreme end of the continuum are major departures from the status quo like new 'champion rules' that essentially close markets to foreign competitors."

BREACHES OF CONTRACT, EXPROPRIATIONS, AND DEFAULTS

"A 2004 World Bank study found that 15 to 30 percent of contracts in the 1990s involving $371 billion of private infrastructure investment were either renegotiated or disputed by governments." Some countries may be unable to pay their debts; others are merely unwilling, perhaps swayed by domestic politics, as in the cases of Russia in 1998, Ecuador in 2008 and Greece in 2015. "National decisions about economics are never just about economics."

CORRUPTION

"The World Bank broadly defines *corruption* as 'the abuse of public office for private gain,'" and in many parts of the world, such abuse increases the cost of doing business by 10 percent. "Emerging markets are particularly prone to corruption" due to their interdependent economic and political spheres and weak institutions, where laws are enforced inconsistently and unpredictably.

Corruption is unavoidable and exists in some form in every country in the world, making the incentives to play in a rigged system highly attractive. But the risks are obviously huge, especially under the U.S. American Foreign Corrupt Practices Act and the U.K. Bribery Act 2010, two laws with extremely broad reach.

EXTRATERRITORIAL REACH

The laws of one country can extend deeply into the activities and affairs of other countries, as evidenced by the 2015 arrest and prosecution of FIFA officials charged with violating U.S. anticorruption laws, as well as the "311 sanctions" that the U.S. Treasury Department can impose on financial institutions linked to money laundering anywhere in the world. Such sanctions can have long-lasting signaling effects, even after the freeze is lifted.

MANIPULATION OF NATURAL RESOURCES

In the 1970s, OPEC's oil embargo on Israel's allies drove up prices around the world, triggering stagflation in the U.S., Europe and Japan. It also led to the discovery of new sources of petroleum, investment in alternative energy sources and new fuel efficiency standards. Today, China produces "more than 90 percent of the seventeen rare earth minerals … [that] are vital components in most high-technology devices." Just as OPEC countries did in the 1970s, Beijing uses its control over these precious resources as leverage in myriad ways.

SOCIAL ACTIVISM

"Technology-empowered social activism offers enormous potential benefits, enabling citizens to mobilize against repressive regimes, fostering greater democratic transparency and responsiveness, and bringing companies and stakeholders closer together. But it also poses new challenges." Dedicated activist groups such as Greenpeace now have far wider reach than before, as do ordinary consumers, armed with nothing more than access to social media. But with the risk comes incredible opportunity as well, as Procter & Gamble learned from its Always-branded "Like a Girl" campaign.

TERRORISM

"Terrorism has become a growing economic and security concern for governments, particularly in Europe. In 2015-16 the Eurozone saw a record number of successful and foiled terrorist plots." Such attacks "often trigger cascade effects for specific companies that can be widespread, long-term, and surprising." The effects of the 9/11 attacks, for instance, while direct and immediate for many companies, took much longer to become fully clear for others.

CYBER THREATS

While the actual cost of cybersecurity breaches is hard to quantify, one estimate puts it at $575 billion per year, including "everything from customer notification, forensic investigations, legal fees, and fines to lost business and long-term reputational damage." State-sponsored hackers and politically motivated hacktivists break into and disrupt government systems all around the world. Companies both large and small are at risk, and any device connected to the internet is a potential access point. Sony's 2014 breach—attributed to the North Korean government—was ostensibly over the release of a film lampooning Kim Jong Un, but "became a national security incident involving the highest levels of the U.S. government" that "erupted into an international crisis."

RISKS FROM WITHIN

Yet it's also "important to underscore that sometimes the biggest political risks come from within. Organizations can hurt themselves by paying too little attention to their own corporate cultures and practices," as both Fox News and Uber learned from their respective sexual harassment scandals. "For both companies, these 'sudden' crises were self-inflicted and years in the making."

03

CHAPTER THREE

HOW WE GOT HERE: MEGATRENDS IN BUSINESS, TECHNOLOGY, AND POLITICS SINCE THE COLD WAR

In February 2014, Joseph Estrada, the mayor of Manila, banned cargo trucks on main roads throughout the city from 5 a.m. to 9 p.m. The daily movement of 6,000 shipping containers was reduced to 3,500. Global automaker Toyota experienced a 10 percent decline in shipments from the Philippines, due in part to Mayor Estrada's ban. "Toyota's cargo container woes in Manila illustrate just how much business has changed, even for traditional industries like automotive companies."

BUSINESS TRENDS: GLOBALIZATION AND SUPPLY CHAIN INNOVATION

"Today's supply chains are longer, leaner, and more global than at any time in history. Even very small businesses can have long global supply chains, enabling them to seize opportunities and profits by taking advantage of lower wages offshore, low shipping costs, and better inventory management to customize products for different segments." One such company, Dutch smartphone maker Fairphone, "carefully selects its Chinese production partners based on their willingness to uphold various social and environmental practices and works closely with local partners in Africa to ensure that Fairphone is using conflict-free minerals and metals in its phones."

Supply chains have also been pared down, with companies making marginal savings with just-in-time inventory management and storage. But this also makes them more fragile. "In 2014, for example, China moved an oil rig … 70 miles inside Vietnam's exclusive economic zone." This set off protests and led to the shuttering of several factories producing goods for Nike, Apple, Walmart and Target. "What began as a conflict over disputed territorial waters between China and Vietnam quickly ended up affecting store shelves in American cities." Other times, the effects are seen further down the road, as when 9/11 led to the downsizing of airplane parts suppliers, which six years later would throw a wrench into Boeing's $136 billion Dreamliner production.

But, "the most important thing to remember about supply chain vulnerability to political actions is cumulative risk: The risk of disruption in any one node of a supply chain may be low, but the *cumulative risk* of disruption across the entire supply chain is much higher." This means that companies should pay attention even to events that seem unlikely to happen and prepare accordingly. Dozens of events that were considered highly unlikely, from Brexit to the election of Donald Trump as president of the U.S., occurred in 2016 alone.

Natural disasters can wreak havoc on modern supply chains. "Taken altogether, supply chain interruptions from rare events turn out to be not so rare after all. As the saying goes, lightning does not strike in the same place twice. But it does strike someplace nearly all the time."

Many businesses lack full visibility into their supply chains. Boeing, in fulfilling orders for its 787 Dreamliner, created a tiered system of first-, second- and third-degree suppliers. But when third-degree subcontractors failed to report delays and hiccups in production in an accurate and timely manner, the whole system was disrupted. "As of February 2016, Boeing had fulfilled only 380 of the 1,143 orders placed since 2004."

Geography is another factor in the increasing prevalence of supply chain disruptions. To save costs, many companies are integrating labor into their supply chains from countries such as Bangladesh, Indonesia and Brazil, which are more prone to civil unrest, natural disasters and other political risks. These companies are often ill prepared to manage the disruption that can arise from these events, and they lose income as a result.

SMALL GROUPS, BIG EFFECTS: THE RISE OF CONNECTIVE TECHNOLOGIES

In the past, the cost of collective action was very high. "Connective technologies, however, have sent the costs of collective action plummeting, making it much easier, safer, faster, and cheaper for like-minded people to find one another, share information, organize, and take individual actions in loosely coordinated ways toward a common goal, even across vast geographical distances."

In 2011, the self-immolation of a single Tunisian fruit seller named Mohammed Bouazizi set off massive unrest across the entire country and the region, ultimately called the Arab Spring. In 2013, the Rana Plaza factory in Bangladesh collapsed, killing more than 1,100 workers and leading to intense scrutiny and a new commitment to better safety practices across suppliers to global companies, such as H&M, Walmart and The Gap. The LEGO Group ended a 50-year partnership with Shell after a video by Greenpeace shaming the company went viral, demonstrating that effects can even cut across industries.

KEY TRENDS IN POLITICS SINCE THE COLD WAR'S END

"Security is not just about security anymore. International economic challenges have become tightly connected to security politics. States, led by China, are playing a more direct role in the world economy, investing in the infrastructure of other countries, making strategic investments using sovereign wealth funds and state-owned enterprises, and purchasing other governments' debt." Sanctions are now a well-used tool in foreign policy: Prior to 1990, the U.N. had only imposed sanctions twice. Since then, it has done so more than 20 times. Another telling metric: "The G-7 has become the G-20."

Rice and Zegart list four major events that illustrate how the world has changed. First, the 9/11 attacks proved the threat that small, organized nonstate actors can pose to countries even as powerful as the U.S. Second, the 2008 financial crisis showed how international economic factors can be made personal. "When you lose your house because of the global financial system, international economics becomes personal." Third, the Arab Spring has created strife throughout the

Middle East and displaced millions of people, the effects of which are now starting to be seen in Europe. And finally, Russia and China have become more assertive world powers in recent years. China presents particularly thorny challenges, with its enormous global economic and political importance.

Alongside these four shocks, the international system has seen "the growth of populism and protectionism as significant political forces." After World War II, the U.S. and its allies worked hard to create a more open, just, globalized world, helping to establish institutions such as the World Bank, the International Monetary Fund and the World Trade Organization. "But nativism, populism, protectionism, and isolationism are making a comeback." In the 2016 U.S. presidential election, no major candidate defended free trade, Rice and Zegart note. "The risks to a system that for several decades has moved in the direction of openness and freer trade should not be underestimated, by citizens or businesses alike."

04 CHAPTER FOUR

MIND GAMES AND GROUPTHINK: WHY GOOD POLITICAL RISK MANAGEMENT IS SO HARD

"Studies repeatedly find that companies know they are not as good as they should be at political risk management." Many companies have created "political risk units whose mission is to identify political risks and opportunities and to work hand in hand with business unit leaders to mitigate losses and seize new opportunities." Rice and Zegart have identified five factors that make managing political risk difficult, calling them the Five Hards.

1. HARD TO REWARD: "NOBODY GETS CREDIT FOR FIXING PROBLEMS THAT NEVER HAPPENED."

Being the brake on a business plan is a hard job, "particularly if the immediate economic case looks promising and the political risk may be longer-term or harder to see." One risk manager told the authors, "Our measure of success as a political risk unit is whether we have a seat at the table, whether business units are making informed decisions based on our professional expertise." Stanford professor Bill Perry—former U.S. secretary of defense—has found one big reason why defense secretaries fail: "They would not accept opposing points of view, and when they heard one, they would come down very hard on the person providing it."

Risk management can also be a hard sell because its functions incur costs while producing no revenue, and so "business leaders have a hard time knowing whether all these costs are 'worth it'; political risk management often entails anticipating bad things and taking action so those bad things never actually occur." Discerning whether a particular measure prevented disaster is often impossible, making it difficult to reward precautionary actions.

2. HARD TO UNDERSTAND

"Americans are far more afraid of dying in a shark attack than in a car accident, even though fatal car crashes are about sixty thousand times more likely," an example of the way in which humans tend to miscalculate probability. Psychologists Amos Tversky and Daniel Kahneman have studied "common mental shortcuts, called heuristics, that often make decision-making easier and more efficient but can lead to serious errors." One such cognitive bias is the "availability heuristic," in which "people tend to judge the frequency of an event based on how many similar instances they can readily recall." Memorable events—like shark attacks, Ebola outbreaks and plane crashes—are thus deemed more probable than they actually are.

People are also more likely to overestimate the likelihood of outcomes that they find desirable, known as the "desirability" or "optimism" bias. This has applications for everything from sports fans predicting their teams being more likely to win than they actually are to widespread shock over the Brexit referendum, in spite of the polls remaining relatively even leading up to the vote.

Political risks are also "susceptible to being considered in isolation, making them appear to have lower probabilities than they actually do over the longer term or in the bigger picture." For instance, news coverage of terrorism tends to focus on only a few geographic areas, but 47 countries reported 10 or more terrorist attacks in 2014. "The first step toward good political risk management is being brutally honest about the political risks your business confronts. Understanding risks requires overcoming blind spots."

3. HARD TO MEASURE

Political risk is hard to quantify. "It requires a sense of the corruption, regime stability, policy stability, social cleavages, the national mood, cultural norms, geopolitics, domestic politics, and the motives and capabilities of everyone from national leaders to neighborhood associations to nongovernmental organizations and transnational groups." And perhaps the most difficult thing to discern is political intention. Sherman Kent, a Yale professor and a founding father of the CIA, divided information for intelligence analysis into three categories: 1) verifiable facts, 2) knowledge that is knowable but currently unknown by the organization and 3) information that is not knowable to anyone (i.e., intentions and potential future decisions).

There are always two components to consider: "the likelihood that an event will transpire and the expected impact if it does." Since risk analysis and assessment most often involve using past behavior or data to anticipate what will happen in the future, these exercises often lead away from looking at outliers, and "low-probability/high-impact events are especially tricky." Major political events—on the level of a country developing nuclear weapons and incurring sanctions—are called "black swans." But while it may be tempting to dismiss black swan events as essentially random and impossible to predict, there are three things to remember: "1) Political events are man-made, not acts of God; 2) political events require people acting in some sort of concert, and this can leave telltale signs for those who are paying attention before major events arise; and 3) with political events, anticipating directionality is often enough."

4. HARD TO UPDATE

Even after investments are made, companies should continue to update their risk assessments. "Companies often fail to ask, 'What's changed?' before it's too late," which is backed up by Eurasia Group President Ian Bremmer, who found that "while 69 percent of firms analyzed political risks for a new investment, only 27 percent monitored political risk once the investment had been made." At the same time, there is a danger of crying wolf: "Risk updates have to strike the balance between too little warning and too much."

5. HARD TO COMMUNICATE

Like most things, political risk analysis benefits from effective communication. Rice and Zegart have an exercise they use in their class to illustrate the point: “Imagine we offered you a pill that would enable you to look your very best for the rest of your life. … If you took our pill once, you could keep that look for the rest of your life. The pill is guaranteed to be 99.9 percent safe, with no side effects.” Most students raise their hand, but when the pill is instead advertised as killing one in 1,000, very few people volunteer—even though the two scenarios are statistically the same. The takeaway: “The same person will make a very different call depending on how a risk is presented.”

Add to the mix that two people can see the same set of facts and come to completely opposite conclusions based on their own experiences, assumptions and biases, and you begin to understand the inherent challenge of communicating risk.

05

CHAPTER FIVE

MOVING BEYOND INTUITION: OUR POLITICAL RISK FRAMEWORK

This chapter begins the second half of the book, which encompasses the explanation of the four-stage framework for managing political risk that Rice and Zegart have developed. “The basics come down to four core competencies: *understanding* risks, *analyzing* risks, *mitigating* the residual risks that cannot be eliminated, and then putting in place a *response* capability that enables effective crisis management and continuous learning.”

POLITICAL RISK FRAMEWORK

“All organizations want to manage political risks. The ones that do it well work hard to see risks coming; they’re alert. They deploy resources against priorities. … And they know what to do when bad things happen because they have already stress tested their response systems, incentivized the right people and actions, and created feedback loops for continuous learning.” The authors use two case studies to illustrate their framework: SeaWorld’s handling of the fallout from the documentary film *Blackfish* versus Royal Caribbean International’s decision to dock cruise ships at Haiti following the 2010 earthquake.

ROYAL CARIBBEAN INTERNATIONAL AND THE 2010 HAITI EARTHQUAKE

Three days after a devastating earthquake killed 200,000 Haitians, injured 250,000 more and rendered more than 1 million homeless, a Royal Caribbean International cruise ship docked at a private beach

85 miles from Port-au-Prince; it was one of four that would stop by in the following days. Vacationers swam and relaxed, as the humanitarian crisis was still unfolding in its early stages. The immediate public response was extremely vitriolic, with the company's decision depicted as callous at best. But when the news broke that the Haitian government had asked the cruise line to dock there, and the ship was able to offload emergency supplies and resources, the tide of public opinion turned back in favor of the company.

Royal Caribbean International "did much more than execute a crisis response plan well. It took political risk management seriously years before the earthquake struck." For decades, Haiti has been stricken by political instability and incredible poverty. But in the 1980s, "Royal Caribbean International began a long-term relationship with Haiti to develop a private, gated luxury beach destination there." The selected location was Labadee, a remote location in desperate need of cleanup and development. Initially, local residents were resistant, suspicious of the company's motives and skeptical that they would receive any of the benefits. Peter Whelpton, an executive with the cruise company, convened a town hall for locals, aided by his friend Pierre Chauvet, a Haitian involved in the country's tourism industry. There, he promised the development would include an area for Haitian merchants and create new jobs for locals. In addition to the jobs and a per-guest tax paid to the government, the company would eventually contribute $55 million to the nation.

When the earthquake struck, the company tapped into its existing network to make the decision to continue stopping at Labadee. It also "immediately announced it was donating $1 million in aid, bringing hundreds of pallets of relief supplies on its cruise ships, and donating all Haiti shore excursion proceeds to earthquake relief." The company's efforts did not stop even after the press had died down. "Six months after the earthquake, the company announced that it was building a new school in Haiti … and launching 'voluntourism' excursion options for passengers to engage in community service projects while stopping in some of its locations," illustrating its commitment to maintaining the relationship with Haiti and to managing its political risks there.

SEAWORLD'S *BLACKFISH* CRISIS

When negative attention and the withering eye of the public turned to SeaWorld after the release of the critical documentary *Blackfish*, the company was utterly unprepared. "The '*Blackfish* effect' caught on in large part because SeaWorld never built a reservoir of trust with animal rights activists, researchers, political leaders, or others who could have come to the company's defense and stopped the crisis from getting worse." What started out as a PR nightmare soon became a legislative one, as restrictive state and federal regulations began to pass; SeaWorld lacked the political influence to block them. A social media campaign totally backfired.

After three years, new CEO Joel Manby seems to have begun a turnaround. He "announced that SeaWorld was ending all of its orca breeding programs across the United States, phasing out its theatrical orca shows, and dedicating $50 million to a new partnership with the Humane Society of the United States to create educational programs, rescue animals, and combat commercial whale and seal fishing." But the company's future is still uncertain.

WHAT ROYAL CARIBBEAN INTERNATIONAL DID AND SEAWORLD DIDN'T

Royal Caribbean International successfully implemented the four-stage political risk framework by *understanding* and *analyzing* the risk in Haiti early on. Its *mitigation* efforts included gaining trust at the local level and fostering a robust relationship with the Haitian government, international NGOs and the U.N.; building physical safety infrastructure to protect passengers; and diversifying the business, making Labadee just one stop of many. The company's *response* plan was also noteworthy. Its "actions were not misconstrued for long: [COO Adam] Goldstein quickly and clearly communicated what mattered to him and why. He put a human face on this human tragedy, explaining in media interviews and on his own blog what exactly the cruise ships were doing in Haiti and why it mattered."

SeaWorld, by contrast, struggled at every stage of the framework. The company had seen orcas harm or kill trainers and had tweaked safety practices over time, but it had never prepared for the day when those mishaps would become a PR or business crisis. “Although SeaWorld *understood* the safety risks posed by human-killer whale interaction early on and took steps to address them, the company apparently never *analyzed* that the risk of trainer injury or death could jeopardize its core business.” It had an incident reporting system in place, but it was voluntary and incomplete. The deaths of trainer Dawn Brancheau and another were never even reported as “incidents,” perhaps because there was strong pressure from management to keep shows going. Two trainers who stopped a show in 1999 due to an orca’s erratic behavior were actually criticized by Michael Scarpuzzi, VP of animal training.

Blackfish did not come out of nowhere: “Gabriela Cowperthwaite had asked SeaWorld executives to be interviewed for the film, but the company had refused. Similarly, animal rights groups had been criticizing the theme park for years.” But the company did not attempt to *mitigate* any of these risks “by diversifying its revenue sources or attractions, dramatically improving safety, or aggressively pursuing a strategy to build goodwill among external stakeholders—all steps the company began to take after the crisis hit.” But by then, it was too late. SeaWorld’s *response* to the crisis—a defensive letter sent to film reviewers—also backfired, by calling wider attention to the documentary than it might have received otherwise.

In short, “Royal Caribbean International and SeaWorld stories both confronted sudden crises that went viral. Political risk management helps explain why one recovered quickly and the other did not.”

06

CHAPTER SIX

THE ART OF BOAT SPOTTING: UNDERSTANDING POLITICAL RISKS

In 2006, engineer by training and 25-year veteran of LEGO Hans Læssøe decided to build a political risk strategy playbook for the company, which was struggling at the time. He quickly put together a team of the company’s best critical thinkers and brainstormed with people from across the company’s functions to determine the top 100 risks. Then, with two executives, he assigned likelihood and potential financial impact to each risk. “Finally, Læssøe’s team went back to senior managers who needed to ‘own’ each risk to get their feedback, ideas, and buy-in about risk identification, prioritization, and mitigation strategies.”

Læssøe calls this work “‘boat spotting’—identifying big emerging challenges before you miss the boat.” To get better at boat spotting, start by looking within your organization. “Companies that understand risks well develop a common language for seeing and discussing risk systematically. They evangelize the importance of setting the risk appetite and owning risk across the company. And they work to harness creativity, perspective, and truth-telling to reduce blind spots.”

UNDERSTANDING POLITICAL RISK: THREE KEY QUESTIONS

1. WHAT IS MY ORGANIZATION'S POLITICAL RISK APPETITE?

"Companies that manage political risk well start with a grounded general understanding of what risks they are willing to accept. ... Their risk appetite is explicit, updated, widely known, and closely tied to business strategy." The return on any given business decision depends on several factors, including: 1) time horizon (how long it will take for an investment to pay off); 2) alternatives (what other investments a company is considering); 3) ease of exit; and 4) visibility to customers (how political risks might become reputational risks or damage key relationships).

Keep in mind that risk appetite also varies by industry. For example, NASA's crash rate is much higher than that of commercial airlines—in part because we accept that going to space is more dangerous. Consumer-facing companies and industries must worry about reputational risks. Manufacturers are vulnerable to labor disputes. Apparel companies must consider human rights conditions in their factories, often in the developing world. The list goes on. Disney represents one company with a zero-risk strategy, which it believes keeps its brand—its most valuable asset—as safe as possible.

Risk appetite also varies from person to person. "Research has found that these differences in risk tolerance tend to be innate and lasting," with genetics explaining as much as 55 percent of any given individual's risk appetite. In their class, Rice and Zegart have run a simulation exercise for five years about a fictional cruise line's decision to protect itself against the risk of "wrong-place/wrong-time" crimes against passengers in Mexico. Through the years, they have discovered wide variance in the measures taken by each team of five students, which have ranged from keeping itineraries the same with added security measures to withdrawing from the Mexican market entirely.

"Companies, like individuals, often see the same risks differently." For example, in 2011, both ExxonMobil and Royal Dutch Shell signed agreements with the Kurdish regional government in northern Iraq. When Baghdad threatened to cancel contracts in the south over the agreements, ExxonMobil held fast, but Royal Dutch Shell pulled out of its agreement with the Kurdish government. There's no right answer. "The most important thing about risk appetite is that you know what it is."

Stating your risk appetite explicitly is a good idea for three reasons. First, "human cognition is a tricky thing; even when we have the same concrete facts, we can and do interpret them differently." Second, "new people are always entering an organization, and they may walk in the door with a very different understanding of what the company's risk appetite is or what it should be." Last, "risk is dynamic. It is always changing, and a company's risk appetite may shift with it."

2. IS THERE A SHARED UNDERSTANDING OF OUR RISK APPETITE? IF NOT, HOW CAN WE FOSTER ONE?

It is not enough for leadership to be on the same page about risk appetite. "*Everyone* needs to know it. … If political risk management is the responsibility of just the 'risk people,' you'll be in trouble." The best companies make sure "everyone shares a *common language* for discussing risk, a *consistent and repeated process* for identifying risk, and a *sense of ownership* about risk." Paychex, for example, hosts an annual "Tournament of Risk," similar to the NCAA men's college basketball March Madness tournament. The top 64 risks are pitted against each other, and leaders throughout the company vote on the risks they see as the most important. At the LEGO Group, risk management training is required for all project managers.

What these companies have in common is "buy-in from the top about the importance of understanding and managing political risk, practices that create shared knowledge of the company's risk appetite, and a system that ensures there is focused responsibility for owning specific risks."

3. HOW CAN WE REDUCE BLIND SPOTS?

"There are three ways that organizations—from toy companies to spy agencies—reduce blind spots and better see risks around the corner: imagination, walking in the shoes of others, and processes that prevent groupthink at the top."

Imagination: Lessons from *Star Trek*

In the television and film franchise *Star Trek*, "Captain Kirk is the dashing, maverick captain of the starship *Enterprise*. Kirk is creative, unorthodox, and emotional." By contrast, his No. 2, Lieutenant Commander Spock, is devoid of emotion, relying on data, logic and convention to make decisions. "This make-believe dynamic duo conveys a real-world message: Kirk and Spock are far more effective together than they are apart. The same is true with risk identification and analysis."

Risk analysis is Spock, revolving around "hard-nosed, unsentimental analysis of facts." Risk imagination is Kirk, recruiting "creativity, emotion, and thinking about what could be, not just what is." One without the other will never get you far. "Understanding risks as a first step is an exercise in imagination." As Tom Hill, vice chairman of Blackstone Group, says, "The biggest mistake is believing the future will look like the present. It almost never does." He and his team are thus "always thinking about what could change in the world that would affect Blackstone's investments."

FedEx founder and CEO Fred Smith took inspiration for his own board from his experiences serving on the board audit committees of other companies. LEGO uses Google Trends to try to get ahead of risks and opportunities. Paychex's "Tournament of Risk" uses gamification to drive engagement. Many other organizations use scenario planning and war games.

Walking in the Shoes of Others: Lessons from Labadee

"Trying to imagine any particular risk or situation from another stakeholder's perspective can help uncover hidden risks before they become a problem." For Royal Caribbean International's project in Labadee, Peter Whelpton worked to understand why local Haitians were skeptical and address their concerns, thereby ensuring that the company was giving back to the community, not just taking from it. In 2014, a Malaysian airliner was shot down over eastern Ukraine. Many at the time faulted the Ukrainian government for refusing to shut down airspace. But a risk officer whom Rice and Zegart spoke with offered an explanation: To shut down airspace would have required the Ukrainian government to acknowledge that it did not have control of the situation. Understanding the government's decision-making process led some airlines to proactively stop fights anyway, which may have saved lives.

Preventing Groupthink: Lessons from the Secretary of State

"It is also important to create strong channels for dissenting views, new information, difficult feedback, and unconventional thinking to get to the top. Those who use these channels also need to be rewarded." In 2007, a new law made government-issued IDs mandatory for those traveling between the U.S. and Canada. This created a spike in demand for new passports, and the U.S. State Department fell six months behind. What Rice, who was secretary of state at the time, didn't anticipate was that people would renew their passports early, creating even more stress on passport processing.

"Looking back, she wished she had directed someone to stay on top of the passport process every couple of weeks after the law was first passed. … 'I wish the people who had run the passport office had told me they were behind. I could have gotten more resources on it earlier to help solve the problem,'" she says. "The most important thing to remember is not to isolate political risk from the senior levels of the organization."

07

CHAPTER SEVEN

ANALYZING RISKS LIKE A PHYSICIST

In Rice and Zegart's class, they propose a fictional case study in which a Japanese telecom company strikes a deal with the Burmese government to open operations in the Rakhine State. In the scenario, violence breaks out when extremist Buddhists attack the company's Muslim workers. Students must work through how the fictional company can navigate this crisis. From it, they learn three important lessons.

The first lesson is that while quantifiable, national-level data is tidy and often feels "solid," these sorts of data are often not very good at shedding a light on political risk. "People find hard numbers alluring and reassuring," but assessing risk requires turning to qualitative data and analysis. In the case study, students discover that while the Burma telecom market looks ripe for investment on paper, the Rakhine State is one of the most politically and socially volatile regions in the country.

"The second lesson is that political risk analysis should not stop once an investment begins." This is something that even real executives and organizations sometimes fail to understand. "Especially in today's environment, political conditions change, sometimes quickly. Good political risk analysis is ... a continuous endeavor."

Finally, students learn to recognize optimism bias. "Most students walk into class enthusiastic about Burma, seeing a rare opening and a historic business opportunity," only to realize that there are almost always trade-offs to be made and risks to be mitigated. "Integrating political risk analysis into business decision-making helps guard against optimism bias."

1. HOW CAN WE GET GOOD INFORMATION ABOUT THE POLITICAL RISKS WE FACE?

When it comes to analyzing facts, context matters. "Identifying what constitutes 'good information' is itself an act of judgment. What you find depends on what you seek. Three rules of thumb are useful."

RULE 1: GOOD INFORMATION IS SPECIFIC, NOT GENERIC.

Good information "helps answer the question, 'What are the political risks to my organization from this place at this particular time?'" No two organizations will have the same risk appetite or considerations. "Country reports, corruption indices, global industry analyses, and other generic products are fine places to start analyzing risks, but poor places to end." For instance, corruption within any given country varies by region or state, nuance that a report detailing corruption across the world will not contain. Other reports may have more detail but focus on data from one point in time, providing little information about trends or failing to keep up with the often rapid pace of our modern world and its politics.

The good news is that creating your own risk data practice need not require a large amount of staff or funds. Marriott International, a pioneer and leader in global political risk management, has just two full-time professional intelligence analysts. Business leaders can go a long way simply by traveling to sites to see for themselves, as well. "The best information about political risks in the field often comes from visiting the field."

In returning to the original question, note that the question is about political risks *from* any given place, rather than *in*. This wording is intentional; it emphasizes that political risk is rarely, if ever, contained. In fact, it usually cascades outward, far beyond where any single event occurs. "Corruption is the most obvious cascading political risk," with the U.S. and the U.K. both having strict and far-reaching anti-corruption laws.

RULE 2: GOOD INFORMATION INCLUDES PERCEPTION AND EMOTION.

"Perception and emotion are tightly intertwined drivers of human behavior," so good information should include them. In 2006, Dubai Ports World acquired London-based Peninsular and Oriental Steam Navigation. This gave the UAE government-owned company operating control of several ports in the U.S., which required government approval. The Committee on Foreign Investment in the United States, composed of several federal agencies, unanimously approved the deal. Congress, however, had other plans: The House Appropriations Committee voted 62-2 to block the deal, citing security concerns. No amount of rational discussion or analysis could change the members' minds.

"Good information includes gathering a sense of the heated feelings and passions of key audiences. Think of 'perception information' as anything that helps put a finger on the pulse of a group critical to your business."

RULE 3: GOOD INFORMATION COMES FROM ASKING GOOD QUESTIONS.

In 2011, a 9.0 magnitude earthquake struck Japan. The Fukushima Daiichi Nuclear Power Plant shut off its reactors. When it lost electricity, backup diesel generators kept the reactors stable. Then a tsunami knocked out the generators, and two reactors suffered a partial meltdown. After the fact, many assessed the situation as an impossible-to-predict black swan.

But Stanford's Rod Ewing suggests the question that should have been asked: "What if I have a string of reactors along the eastern coast of Japan? What is the risk of a tsunami hitting one of those reactors over their lifetime, say, 100 years?" The likelihood, when analyzed that way, is much higher. Japan had 54 nuclear reactors, and the country is located "in the Pacific 'Ring of Fire,' where 90 percent of the world's earthquakes originate." But coming to this conclusion requires asking the right question and framing your risk analysis correctly.

2. HOW CAN WE ENSURE RIGOROUS ANALYSIS?

"The goal of political risk analysis is not to predict the future. Nobody can do that. The goal is to create better decisions for your organization by developing insight about key drivers and possibilities."

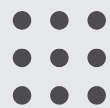
TRAPS

Chapter 4 discussed the pitfalls of the "availability heuristic" and optimism bias, where events that are easy to recall or favorable to us are deemed more likely, respectively. Add to this list mental mind-sets, "unconscious analytic frames used to organize information and make sense of complexity. While frequently useful, mind-sets can also distort thinking in hidden ways."

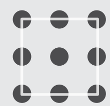
THE NINE-DOT EXERCISE

The nine-dot exercise challenges people to think outside of their automatic assumptions, which are "formed by many inputs—past experience, cultural norms, organizational standard operating procedures, situational context, education, and training. Recognizing them is the first step toward overcoming them."

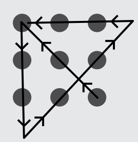
The nine dot exercise



Instructions: Without lifting your pencil from the paper, draw no more than four straight lines that cross through all nine dots.



Many people find this difficult because they assume they cannot let the pencil go outside an imaginary square around the dots.



However, once you discard the assumption of equal line length, it should be pretty easy to draw the four-line answer.

Group dynamics can also pose great challenges. "Nobody wants to be seen disagreeing with the boss. Many bosses do not like to hear dissenting views. Hierarchy and status often stifle discussion of vital information without anyone realizing it." In his book *The Checklist Manifesto*, physician Atul Gawande details how hospital surgical staff members combatted these risks just by introducing themselves to one another before each operation.

But "research finds that even when dissenting views are encouraged, there are strong psychological pressures toward conformity," which can be driven by individuals' desires to preserve group cohesiveness at the expense of a more well-informed decision.

SCENARIO PLANNING

In 1965, Royal Dutch Shell tapped Ted Newland to start a unit called Long-Term Studies at the company's London headquarters. Newland and his colleague, Pierre Wack, created two scenarios for the price of oil: "a stable price scenario and a drastic price change scenario. The stable price scenario was eventually called 'the three miracles' because its occurrence hinged on wildly optimistic exploration and production; all major countries' willing depletion of their hydrocarbon resources to meet consumer demand; and no major supply or demand changes."

Newland and Wack didn't know when the price would go up, but their scenario planning proved that it was more likely than Shell executives had previously thought. In 1973, OPEC suddenly boosted oil prices, proving the pair correct. Below are their top tips for effective scenario planning:

1. Effective scenario planning does not predict the future. Instead, it imagines equally plausible possibilities to stimulate thinking about forces driving the system, their connections, and uncertainties.
2. It deals with both facts and perceptions.
3. It identifies the underlying technological, business, political, and societal forces driving your business.
4. It organizes information into three or four stories of alternative future worlds, each meticulously researched and intended to catalyze "unexpected leaps of understanding."

5. It draws on diverse views, including from unconventional sources.
6. It connects tightly with business strategy and the concerns of managers.
7. It includes opportunities, not just threats.
8. It uses narratives and language to get managers' attention, interest, and buy-in.

RED TEAMS, DEVIL'S ADVOCATES, THINKING BACKWARDS, AND OTHER TOOLS

Scenario planning need not be the only tool in your toolbox. LEGO uses computer simulations. Paychex has their "Tournament of Risk." Many organizations, including U.S. Strategic Command, use roleplaying and war game exercises. Others use "'red teams,' people assigned to assume the role of competitors or adversaries." Regardless of the specifics of the exercise, all red teams "are designed to push insiders to 'think like the enemy.'"

But not all risk management tools require extensive commitment of both staff and money. "Thinking backwards is an exercise that starts by imagining that a surprising and significant future event has transpired. Your job is then to look back from this future and understand how the event could have come to pass. Like scenario planning, thinking backwards is not designed to predict the future." It is an exercise meant to shift thinking out of cognitive traps. "Devil's advocates can be a 'quicker and dirtier' version of red teams," an everyday version of thinking from different perspectives.

3. HOW CAN WE INTEGRATE POLITICAL RISK ANALYSIS INTO BUSINESS DECISIONS?

"Companies that manage political risk well go out of their way to integrate political risk analysis into the everyday rhythms and decisions of the business." At LEGO, Hans Læssøe made sure that strategic risks were owned by people throughout the organization. He "created a database and risk process that every project manager could easily use, and he created training in risk management for them all." He also made it a point to organize his job under the CFO rather than the general counsel, so that managing risk would not be seen as merely a compliance issue. "A second building block in Læssøe's plan was creating a standardized decision-making process that incorporated strategic risk analysis." Called Active Risk and Opportunity Planning, it was "designed to ensure that managers consider both downside risks and upside opportunities."

But across discussions with business leaders who handle risk, Rice and Zegart found that one lesson emerged: "Their most important job is making political risk useful throughout the company. That starts with developing a deep understanding of the business and the needs of managers." After all, "recognizing the incentives, priorities, and perspectives of others does not apply just to external stakeholders." Developing mechanisms to see the different perspectives of all functions ensures that "political risk can be baked into assessing the trade-offs of a business decision, not considered as an afterthought."

08

CHAPTER EIGHT

THE NUCLEAR TRIAD, THE EMPTY PLANE, AND OTHER WAYS TO MITIGATE RISKS

Every night of the year, FedEx flight 1311 flies from Denver to Memphis carrying no passengers. "The plane's role: recovering unanticipated cargo." It is just one of the company's extensive risk mitigation measures. FedEx's Global Operations Control Center, a sprawling 800-acre facility in Memphis where planes land as often as every 40 seconds, is, of course, wired with state-of-the-art technology. But for the company, "risk mitigation is about people and process, not just technology." Each plane is named after a FedEx employee's child, and many leaders started out as package handlers or couriers. "When it comes to hiring, FedEx looks for people who are team players, are adept at evaluating large quantities of information, can make fast decisions, and can stay calm under pressure."

Equally important are well-developed processes. "The center conducts regular training to ensure cool, focused action under pressure," and managers have broad authority to "change flight paths whenever necessary rather than wading through layers of bureaucratic approvals each time. Crisis decision cycles extend over three to four days to limit confusion and improve coordination." The company is always anticipating and preparing for mitigating risk, knowing that risks are unavoidable.

"Success requires a multi-layered approach that uses three interlocking strategies: *developing mitigation strategies in advance*, *creating warning systems that enable fast action when you need it*, and *building resilience so the entire organization can bend without breaking when bad things happen*."

1. HOW CAN WE REDUCE EXPOSURE TO THE RISKS WE HAVE IDENTIFIED?

"Organizations can reduce exposure to political risks in many ways, but every strategy should begin by understanding what most needs protecting. … Risk mitigation requires trade-offs, and trade-offs require understanding what assets are *most valuable and most vulnerable*."

UNDERSTANDING WHERE ASSET VALUE AND VULNERABILITY CONVERGE

"At FedEx, asset value and vulnerability are clear: On-time delivery is the company's holy grail. It is the most important part of FedEx's value proposition and also the most vulnerable." FedEx understands that its business depends on maintaining customer trust, starting from the CEO. Many companies do not understand the convergence of asset value and vulnerability. In the case of SeaWorld, huge portions of its business banked on orca shows and branding. That's why *Blackfish* was able to damage the company's business to the extent that it did. Anything SeaWorld did afterward to recover could have been done beforehand to mitigate the risk in the first place.

"Sketching value and vulnerability along a 2-by-2 matrix helps illuminate risk mitigation priorities. Start by asking:

- What assets are most valuable to my organization?
- What assets are most vulnerable to political risk?
- Where do high value and high vulnerability cluster?"

TWO COMMON MITIGATION STRATEGIES: MARKET AVOIDANCE AND TIMING

Risk mitigation doesn't need to be complicated; sometimes, simply making the choice not to enter a market at all is the right one. In other cases, carefully planning your investment time frame can offset anticipated political risks. Silicon Valley entrepreneur and investor Vinod Khosla once greenlit entrance into a foreign market in spite of a near guarantee of intellectual property theft. "But because the company was estimated to have a ten-year profit window in that market before that occurred, the entry made sense."

BUILD YOUR NUCLEAR TRIAD: DISPERSING CRITICAL ASSETS

American nuclear weapons were split into three components during the Cold War so that no single attack could destroy all of them. "Businesses need to build their equivalent of the nuclear triad to reduce the impact of any single political event on the bottom line. No organization should have its most valuable resources exposed to the same risk at the same time."

Cantor Fitzgerald lost 658 employees at its New York office (nearly two-thirds of its U.S. workforce) in the 9/11 terrorist attacks. Yet just two days later, the firm's services were back up. This was in part because the company had set up three separate data centers for its online trading subsidiary, eSpeed, and its large London office was able to keep the business afloat. "Without a risk mitigation plan that included dispersing key assets, Cantor Fitzgerald probably would not have survived."

FLY THE EMPTY PLANE: CREATING FLEXIBLE SURGE CAPACITY

Although many companies have been rooting out and eliminating slack, it has its benefits. "Without it, unforeseen events … can take a heavy toll." After 9/11, Boeing's 787 Dreamliner production fell behind by three years over fasteners that were 3 percent of the cost of any single airplane, which could have been mitigated by merely having more inventory on hand. "Other firms create flexible surge capacity through standardization or last-minute customization." For example, all of Intel's semiconductor plants are designed identically, so that they can all fill in for one another, if needed.

BAND TOGETHER: ALIGNING WITH OTHERS IN YOUR INDUSTRY

"Aligning with others in your industry takes two forms: sharing information about risks, and pursuing voluntary collective action to preempt more damaging legal or regulatory changes to the industry." Alan Orlob, VP of global safety and security at Marriott, believed that he could differentiate his company's hotels through their best-in-industry security and safety. He succeeded. Unfortunately, terrorist attacks on other Western hotel chains continued, and he decided that collaborating on security was a better idea than competing. "So he established a hotel security working group to share information and best practices among security directors from the ten biggest hotel companies and got the State Department's Overseas Security Advisory Council to sponsor it."

Collective, industry-wide agreements to self-regulate can also sometimes allow companies to prevent stricter third-party regulation. This strategy has given rise to such things as movie ratings and the Kimberley Process for combatting blood diamonds. In response to the Rana Plaza factory collapse in Bangladesh, more than 150 clothing companies agreed to work together to improve working conditions and safety. In all these cases, the goal was "to reduce the probability of more serious regulatory and legal changes and to reduce activist and consumer backlash on salient social issues."

2. DO WE HAVE A GOOD SYSTEM IN PLACE FOR TIMELY WARNING AND ACTION?

The next step is to develop "a warning system to spot residual risks in time to take action." While scenario planning and red team exercises focus on risks on the horizon, warning systems deal with real and present crises. "Effective warning systems do two things well: *provide situational awareness* and *set tripwires and protocols* so that certain steps are triggered automatically when conditions warrant."

SITUATIONAL AWARENESS

"First reports are almost always incomplete. Getting an accurate understanding of a crisis as it unfolds is essential, difficult, and requires robust information sources and coordination." The Situation Room in the White House was created for just this reason. "Today, companies on the front lines of managing global political risk have developed in-house threat assessment units staffed with former intelligence and law enforcement professionals to provide situational awareness about political developments around the world in real time."

"The best in-house risk teams have four core competencies to develop situational awareness:

- An ability to sift through voluminous amounts of information quickly to determine relevant political risks
- A deep understanding of the business to identify quickly what matters most for their bosses
- A forward-leaning entrepreneurial approach to collect and share information that may not be obvious or readily available through standard products
- A healthy skepticism about how incentives might affect what information they receive and when they receive it"

SETTING TRIPWIRES AND PROTOCOLS

"Tripwires are systems that identify what information to look for in advance. Protocols make clear what steps should be taken by whom when the tripwire gets crossed. The idea is to reduce decision-making on the fly." These tools are already common in places such as emergency rooms and aircraft carriers. "To be sure, indicators of political risk are much murkier than indicators of a heart attack or a safety problem on a carrier flight deck. But the basic idea is the same: Organizations that identify warning indicators and reaction protocols are better able to mitigate risk than those that don't."

Here is one of Rice's favorite questions to ask when helping students set up tripwires: "How do you know it when you see it? What evidence would prove your hypothesis right or wrong?" Rather than focusing on current conditions in any given environment, "a better approach is to develop tripwires in advance." In the classroom case study of a cruise line deciding how to mitigate risk of violence in Mexico, students are instructed to identify specific indicators about safety conditions, such as an "overall decrease in cartel-related violence" or "deteriorating relationships with local port security officials."

Tripwires need not be overly complex. "Even basic indicators can help. Identifying what to look for ahead of time helps guard against cognitive bias and makes data gathering and analysis more efficient." And tripwires should be clearly and specifically linked to protocols, ensuring as little delay between warning and action as possible.

3. HOW CAN WE LIMIT THE DAMAGE WHEN SOMETHING BAD HAPPENS?

"The final layer of risk mitigation is damage control. The headline here is to take action before you need to—specifically, by developing relationships and contingency plans."

BUILDING RELATIONSHIPS: DRINK THE CUP OF COFFEE!

"Companies that effectively manage political risks develop relationships with stakeholders early and often." In a critical scene of the film *Erin Brockovich*, Erin and the lawyer she works for, Ed, convince a family to join a class-action lawsuit. On the way out, the family offers the two some coffee. Ed declines, but Erin stops him, insisting that he drink the cup of coffee. She knew that "coffee was not a waste of time. It was a golden opportunity to deepen a personal connection."

Two years before opening up a mine in Brazil, Alcoa carried out a robust campaign to gauge local concerns, hosting discussions and building relationships with local residents, governments and civil organizations. Even after the mine opened, "it established a $35 million development fund for sustainable initiatives proposed by the community." As Adam Goldstein—the executive responsible for Royal Caribbean's development in Labadee, Haiti—puts it, "You make relationships when you want to, not when you need to—because when you need to, it's too late."

CONTINGENCY PLANNING

"Plans are often useless. It's the planning process that is valuable. Plans will almost never match the conditions of the future, but planning builds capacity to succeed anyway by developing what we call the three Rs: *roles*, *repertoires of action*, and *routines of coordination*. Roles clarify who does what. Repertoires provide broad options for what can be done. Routines of coordination determine how it can be done well."

"*Rule 1: Roles should be clear.* By definition, contingency plans are used when normal processes are not enough and conditions are not ideal. … The more that roles are delineated, the faster and better your organization can execute its contingency plan." In a crisis, this saves valuable time.

"*Rule 2: The more repertoires of action, the better.* … Repertoires of action develop fundamental skills for the totally unexpected and provide options that can be used in different combinations and ways." Chess grandmasters are good at chess because of their ability to recognize patterns and compare them to their prepared repertoires of action—not necessarily because they're smarter or more naturally gifted at chess. Likewise, for organizations, "good contingency planning develops broad options as well as fundamental skills that can be deployed to help the entire organization adapt to unforeseen circumstances."

"*Rule 3: Coordination routines are essential.* … Coordination is where roles and repertoires come together. Coordination routines establish trust and patterns of interaction that smooth the functioning of groups under stress. The best way to develop coordination routines is practice." In 1980, Operation Eagle Claw, meant to rescue 53 hostages in Iran, had to be aborted; eight service members died in a collision between two American aircraft. This happened even though each branch of the military involved had no doubt memorized its part. The missing piece was coordination.

This illustrates valuable lessons: "Coordination should never be assumed, even when the stakes are high, the mission is clear, and the will to succeed is shared by all. Coordination does not just emerge organically. It has to be ingrained through practice and supported by leaders at the top." Silos are natural, so "managing political risk is an exercise in silo-crossing."

09

CHAPTER NINE

ZULU TIME: RESPONDING TO CRISES

In July 2009, a double bombing occurred in Jakarta, Indonesia, at both the Ritz-Carlton and JW Marriott hotels. These were two of the most secure hotels in the city, if not the world. But the news coverage painted an inaccurate picture. To correct this, Alan Orlob, VP of global safety and security, began giving interviews. “His message: Marriott security was robust, but the company was committed to conducting a complete review of this attack, and if additional security measures were necessary, they would be implemented.” His interviews changed the narrative.

“Marriott’s experience shows how to handle ‘Zulu time,’ when events erupt and response cannot wait until tomorrow. … Effective communication in the heat of the moment is important. It is never enough.” Here are the key questions to ask and answer.

1. ARE WE CAPITALIZING ON NEAR MISSES?

“The best way to deal with crises is not to have them. All organizations want to learn from failures.” Yet, “not enough try to learn from near misses.” People often “take false comfort in near misses, seeing them as signs of success rather than warnings of potential failure.” As Georgetown’s Cathy Tinsley says, a near miss “can be evidence of a system’s resiliency, or it can be evidence of that system’s vulnerability.”

Misreading near misses can have disastrous consequences, as when NASA ignored warnings of O-ring deterioration in cold weather and cleared the *Challenger* liftoff anyway—resulting in the death of seven astronauts. On U.S. aircraft carriers like the USS *Carl Vinson*, every successful takeoff and landing is considered a near miss—because it is. This “highlights three tips for any organization seeking to learn from near misses.”

TIP 1: PLAN FOR FAILURE, NOT SUCCESS.

“Organizations that learn from near misses are fundamentally pessimistic. They assume that failure is always just around the corner and invest in developing structures, processes, incentives, cultures, and technical tools to prevent it. … In carrier aviation, landings are scrutinized no matter who sits in the cockpit, how many times they have flown, or what the circumstances are.” At Marriott, Orlob had continued to improve and maintain high levels of security at properties in Jakarta despite the fact that there hadn’t been a major terrorist attack in four years. “Organizations that adopt a ‘planning for failure’ mentality are more likely to see near misses, take them seriously, and learn from them.”

TIP 2: LOOK FOR WEAK SIGNALS.

“Anything that does not perform as expected could be an early indicator of a serious problem. Of course, not every weak signal is. That’s why it is important to look deeper, at possible systemic deficiencies, whenever weak signals are found. And then take strong action.” An illustrative example: GE and Honeywell’s merger in 2001 was blocked by European regulators, the first time a major American deal like this hadn’t gone through. But four years earlier, Boeing and McDonnell Douglas’s merger was only barely approved after a series of last-minute negotiations. “Boeing’s 1997 deal was a signal that European regulators would no longer rubber-stamp American corporate mergers” and should have been interpreted as such.

TIP 3: REWARD COURAGEOUS ACTS.

"Organizations that learn from near misses develop cultures that reward courageous acts. … Calling a time out to examine a weak signal is an act of courage. Recognizing those moments can make a difference." On the USS *Carl Vinson*, one seaman lost a small tool. On aircraft carriers, this is a big deal, as anything that could be sucked into a jet engine could easily lead to disaster. The flight deck's operations were completely halted, and hundreds of people manually searched the deck for the lost item. The next day, the seaman was formally recognized.

2. ARE WE REACTING EFFECTIVELY TO CRISES?

No matter what, "big surprises can still occur. Your organization's response determines whether that crisis fades or festers. As Warren Buffett once said, 'It takes twenty years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently.'" Johnson & Johnson's handling of the seven deaths caused by Tylenol tampering in 1982 provides a model even now.

STEP 1: ASSESS THE SITUATION.

"The first step in crisis management is to get a better handle on what is happening. Early moments of a crisis are swirling with uncertainty. … Assessing the situation takes discipline and time. Yet modern communications technologies are straining discipline and compressing time." In cyberattacks, the instinct is to move as fast as possible. Yet "while responding quickly is important, executives today need to resist the urge to respond so fast that they provide inaccurate information, worsen the damage, or make promises about fixes that they cannot deliver."

In the wake of its 2013 breach, Target made things worse by communicating too frequently, often having to correct previous updates. Speed is often important, but not at the risk of accuracy. "The upshot is this: Do not say what you know. You could end up being wrong. Instead, say what values you believe in and what actions you will take to get to the bottom of the crisis while you figure out what is going on."

STEP 2: ACTIVATE THE TEAM.

"In 1982, Johnson & Johnson did not have a crisis response team, so CEO James Burke formed one as soon as the news broke. … Today, no company should be designating a crisis response team or formulating a plan *after* a crisis breaks. Companies should already have a system in place for reporting crises, a plan for gathering and sharing relevant information, and well-defined roles that are updated and practiced. Not everything can be anticipated, but having these basic capabilities in place provides a head start."

STEP 3: LEAD WITH VALUES.

It is easy to start assigning blame in the face of a crisis. But "that is not what customers and other stakeholders want to hear. They want to hear what your company stands for and why. They want to know what you will do to earn back their trust. They want to know that you care, that you are committed, and that you are contrite."

Johnson & Johnson looked to the credo that founder Robert Wood Johnson crafted for the company: "We believe our first responsibility is to the doctors, nurses, and patients, to mothers and fathers and all others who use our products and services." Using this as a guiding principle, Burke led the company to spend $100 million to recall all the Tylenol and develop new tamper-resistant packaging—against the advice of the FBI and the FDA and with disregard to what the recall would do to J&J's bottom line. All of this was done to respond to a crisis that in no way was the fault of the company.

"Johnson & Johnson was a victim of a crime. Most companies facing political crises are not. For them, the lesson … is the power of accepting responsibility. Assuming full responsibility for a crisis, even one not of your making, and demonstrating that your organization truly cares about rebuilding trust can go a long way." United Airlines CEO Oscar Munoz provided a textbook example of how not to respond when he gave an apology that seemed insincere after video footage of a passenger being beaten up and dragged off a plane surfaced. He then doubled down in a letter to employees that called the passenger "disruptive and belligerent."

"The moral of the story is that genuine contrition matters. Corporate crises are ultimately about trust. The best way to restore trust is to own the problem, know your company's core values, and manage to them. That is particularly true today, when polls show that trust in business executives is not much higher than it is in used-car salesmen."

STEP 4: TELL YOUR STORY.

"Taking time to gather facts does not mean that companies should stay silent," however. "They need to tell their story rather than hiding from the press and difficult conversations." Again, FedEx is an exemplar in this area, partially because it is used to dealing with crises big and small in real time: from lost packages to flight path disruptions and the like. But "how can companies in other industries—where the business model does not demand real-time response to customer concerns—handle sudden crises effectively?" They can start "by carefully distinguishing between facts and values. Facts take time to unfold. Values can be communicated immediately."

Marriott's Alan Orlob was able to do this by agreeing to do interviews. He "was careful to avoid speculating or commenting about what could have gone wrong; instead, he focused on communicating his determination to find out and fix it." Third-parties can be helpful in lending credibility to your organization, as well. Haitian official Leslie Voltaire, who was in New York at the time of the 2010 earthquake, was able to help Royal Caribbean by "explaining that the government wanted Royal Caribbean International ships to keep coming" even after the earthquake.

STEP 5: DO NOT FAN THE FLAMES.

"Finally, organizations need to be aware that they are always speaking to multiple audiences. Each can fan the flames, creating new risks and worsening the crisis." For United, the passenger being dragged off the plane started out on social media, quickly moving to mainstream media, drawing congressional attention and spreading internationally, sparking the ire of China, in particular. Remember that anything you say to one audience can and probably will be heard by others.

3. ARE WE DEVELOPING MECHANISMS FOR CONTINUOUS LEARNING?

"Responding well to a crisis in the moment is part of the battle. Developing mechanisms to remember the right lessons from that crisis is another." Almost 20 years after the *Challenger* tragedy, space shuttle *Columbia* suffered a similar explosion, this time due to thermal foam shedding that had occurred during 65 previous shuttle launches. "At first, the shedding was considered dangerous. But the more it happened, the less dangerous it seemed."

Stanford sociologist Jim March has "found that continuous learning involves two skills: 'the exploration of new possibilities and the exploitation of old certainties.' *Exploration* is the search for new ways of doing things. *Exploitation* is the process of implementing them. Exploration and exploitation often compete and conflict." The former is "creative, disruptive, and uncertain," while the latter is "efficient, order-inducing, and predictable. Companies that excel at continuous learning keep exploration and exploitation in productive tension. This is hard to do."

Professional football teams are an exceptionally good, if surprising, example of organizations that do both exploration and exploitation well. "Activities like watching game tape, devising plays to exploit opponents' weaknesses and capitalize on your strengths, and adjusting the lineup for better matchups are exercises in exploration—they are innovations to gain advantage. Activities like practicing hurry-up offense and conducting drills to hone the capabilities of specialized positions, including backup players, so they are ready to substitute in at a moment's notice are exercises in exploitation."

"Continuous learning takes a heavy dose of leadership to work. … Organizations in the real world are filled with people who respond to leaders and values that inspire. Creating mechanisms for continuous learning must involve both the head and the heart."

10

CHAPTER TEN

STRENGTHENING YOUR POLITICAL RISK MUSCLES

“No one can see precisely how human history will unfold. But managing political risk does not have to be pure guesswork. ... Just as world-class athletes enhance their performance through strength and conditioning training, companies can improve their performance by building their all-around political risk muscles. We hope you will think of our framework as a workout plan or training guide to get your organization into better shape.”

“The most effective organizations have three big things in common: They take political risk seriously, they approach it systematically, and they lead from the top.”

Remember: “Bad surprises will always happen. But organizations that take a serious, systematic, and senior-driven approach to political risk management are likely to be surprised less often and recover better. Companies that don’t get these basics right are more likely to get blindsided.”

About World 50

World 50 is the premier resource for senior executives from globally respected organizations to privately and candidly share ideas, solutions and collaborative discovery.

The World 50 community represents more than 1,400 senior executives from more than 700 globally respected companies across six continents. Membership provides unparalleled access to world-class gatherings as well as year-round peer-to-peer and team-to-team collaboration, delivering insights found nowhere else. Intimate participation with remarkable practitioners and expert thinkers creates a candid dialogue on leading and growing significant enterprises in a global economy.

Inquiries? +1 404 816 5559