

Novel Risks

Robert S. Kaplan
Herman B. “Dutch” Leonard
Anette Mikes

Working Paper 20-094



Novel Risks

Robert S. Kaplan
Harvard Business School

Herman B. “Dutch” Leonard
Harvard Business School, Harvard Kennedy School

Anette Mikes
Oxford University

Working Paper 20-094, Revised May 2020

Copyright © 2020 Robert S. Kaplan, Herman B. “Dutch” Leonard, and Anette Mikes.

Working papers are in draft form. This working paper is distributed for purposes of comment and discussion only. It may not be reproduced without permission of the copyright holder. Copies of working papers are available from the author.

Funding for this research was provided in part by Harvard Business School.

Novel Risks

Robert S. Kaplan¹, Herman B. “Dutch” Leonard², and Anette Mikes³

Abstract

All organizations practice some form of risk management to identify and assess routine risks in their operations, supply chains, strategy, and external environment. These risk management policies, however, fail in the presence of novelty. Novel risks arise from unforeseen events, from complex combinations of apparently routine events, and from apparently familiar events occurring at unprecedented scale and speed. Mobilizing routine risk management to novel events will be ineffective, and, more seriously, delude management into thinking that risks have been mitigated when they may already have escalated to serious consequences. Based on best practices from the private and public sector, the paper describes structures and processes to identify and respond to novel risks. A critical incident management team makes assessments and develops options in the event’s uncertain and volatile environment. The team’s decision-making process has to be rapid, improvisational, iterative, and humble since not every action taken will work as intended.

¹ Harvard Business School

² Harvard Business School and Harvard Kennedy School

³ Saïd Business School, Oxford University

Novel Risks

Organizations have well-established policies to anticipate and mitigate the routine risks that arise in their day-to-day operations, supply chains, and product development. Referring to them as “routine” does not imply that they are unimportant, not dangerous, or that they are easy to mitigate and manage. Their “routineness” comes from their familiarity, enabling managers to identify, assess and mitigate them in advance with situation-specific approaches, as described in the Sidebar: Three Types of Routine Risks.

Sidebar: Three Types of Routine Risks

The table below illustrates the three types of routine risks. Routine operational risks include illegal and unethical actions such as bribery, harassment, embezzlement, and code of conduct violations, as well as deviations from standard operating procedures. Strategy risks are those that are inherent to the company’s operations and strategy such as quality and delivery problems supply chains, uncertain outcomes from research and development, interest and credit risk from lending activities, competitor actions, and hazards from challenging and dangerous work environments in industries such as those in chemicals, mining, and energy exploration, production and distribution. External risks occur outside the company’s strategy and cannot be influenced or even predicted by the company. These include natural disasters, economic disruptions, geo-political turmoil, and pandemics. Companies have mechanisms, as shown in the Figure, to mitigate the impact of all three types of routine risks through time-tested risk management processes.

Risk Categories	Controllability and Relationship to Strategy	Risk Management Tools
Operational and compliance risks	Organizations can prevent or cost-efficiently minimize occurrence of risk. There is no strategic benefit from taking these risks.	Internal controls Codes of conduct Mission and value statements Internal and external audits
Strategy execution risks	Taking these risks is essential for achieving strategic returns. Organizations may reduce the likelihood and impact in cost-efficient ways.	Risk identification and assessment with risk maps Risk mitigation initiatives and risk owners Resources allocated to fund the risk mitigation initiatives
External risks	Organizations cannot control the occurrence of such risks, but they can prepare for them and reduce their impact.	Risk envisionment via scenario planning and war games Contingency planning Insurance and hedging programs

Source: Kaplan-Mikes (2011)

Not all risks are routine

Some risk events, however, are “novel,” because they were never envisioned by the company’s routine risk management processes. Three types of novel risks can occur:

- (1) *Black-Swan* events are rare, arising from threats not previously encountered or envisioned. Black Swan events, however, are often more descriptive of the beholder than of the event itself. Many viewed the 2007-2009 Global Financial Crisis as a Black Swan event. Despite this label, several investors and banks did anticipate the possibility of a mortgage market meltdown, neutralized their holdings or sold short mortgage-backed securities, and survived the

event quite well. Black Swan events can arise even during routine operations, such as the small fire in a semiconductor plant described in the SIDEBAR (see SIDEBAR Fire at a Semiconductor Plant). Companies can avoid the worst consequences from a Black Swan events if they are able to envision them in advance, using tools such as scenario analysis. Once envisioned, they can take actions to mitigate some or all of the severe consequences should the event arise, in effect transforming a novel risk into a routine one. Such a process, to identify and manage formerly unaddressed risks, should be an important component within routine risk management.

SIDEBAR Fire at a Semiconductor Plant

In March 2000, a lightning strike triggered a small fire at a Philips semiconductor plant in New Mexico. The fire department arrived soon after and extinguished the minor fire within minutes. The event did not warrant reporting in the local newspaper. The plant manager dutifully reported to the purchasing managers of all companies sourcing products at the plant that a small fire had occurred that caused only superficial damage and destruction of some work-in-process inventory. He assured them that the plant would be back operating in a week. The purchasing manager at Ericsson, one of the plant's principal customers, checked that his on-hand inventory of the semiconductors produced by the Philip's factory was adequate for production needs over the next couple of weeks and did not escalate the issue further, treating it as a normal and minor supply chain disruption.

Unfortunately, the fire's smoke and soot and the fire department's extensive hosing of the facility had contaminated a much larger area of the Philips plant than initially thought, including the clean rooms in which it fabricated highly sensitive electronic parts. The re-start of production was delayed for months and by the time the Ericsson purchasing manager learned about the

extensive delay, all of Philip's alternative production capacity for the wafers had been purchased by Nokia, its principal competitor. Lacking key components, Ericsson's delayed the launch of its next generation phone at a cost of \$400 million in lost revenues, and exited the mobile phone market in the following year. The Ericsson purchasing manager had treated the fire as a routine delay in its supply chain, and did not anticipate the novelty that might arise from the report of a small fire at a distant supplier's location.

(2) *Perfect Storm* events arise in large, inter-connected technologies, systems, and organizations when multiple events, each of which appears to be routine and manageable in isolation, combine to trigger a major failure (See SIDEBAR Boeing Development Projects). A sequence of small failures at the Three Mile Island nuclear plant eventually led to an almost uncontrollable nuclear meltdown.

SIDEBAR Boeing Development Projects

Boeing, in 2003, began the development of an entirely new aircraft, the 787 Dreamliner, which it forecasted would start commercial flights in May 2008. The novelty of the Boeing 787 development included a series of apparently routine challenges that all had to be managed simultaneously. Boeing introduced new structural materials, composites rather than aluminum, for the airframe; required its first-tier suppliers to take on unprecedented responsibility for design, engineering, and integration; and replaced the hydraulic controls used in previous generations of aircraft with electronic controls that required large, lithium batteries for backup. A Boeing engineer observed that, compared to all prior models, the 787

was “a more complicated airplane, with newer ideas, new features, new systems, new technologies.”¹

Boeing eventually announced seven separate and unexpected delays in the 787 product development schedule. The plane, after incurring more than \$10 billion in added costs, and the forced purchase of a major supplier to prevent insolvency caused by delivery delays, eventually began commercial flights in October 2011. After launch, the plane’s on-board lithium batteries caught fire during several flights and civilian aviation authorities grounded all 787s in January 2013. After Boeing revised and tested a new battery design, the 787 resumed passenger service several months later. A senior manager reflected, “We made too many changes at the same time – new technology, new design tools and a change in the supply chain – and thus outran our ability to manage it effectively.”²

In a further instance of failing to manage novelty, Boeing’s engineers, in the subsequent 737MAX plane development, introduced a larger, more fuel-efficient engine. Rather than invest in the design and engineering for an entirely new airframe, the company decided to place the new engine on its legacy 737 platform, which had been originally designed in the 1960s. The larger engine required a different placement on the aircraft’s wing, which affected the plane’s aerodynamics. The project engineers designed special flight control software to counteract the new plane’s tendency to tilt upward, and assumed that experienced pilots would recognize and quickly counteract the occasions in which the software might trigger an incorrect automatic response. In in at least a couple of cases, however, the novel situation of losing tactile control over the aircraft, while alarms were flashing and warning

¹ Gates, D. Boeing celebrates 787 deliveries as program’s costs top USD32 billion. *Seattle Times*. 24 September, 2011.

² “Boeing says learned from outsourcing issues with 787,” *Reuters Market and Finance News* (January 20, 2011).

bells were sounding in the cockpit, immobilized the anticipated responses of otherwise competent and experienced pilots. After two deadly crashes within a five-month span, regulators around the world grounded the plane until the dangerous situation could be properly identified and mitigated, during which Boeing, its suppliers, and its airline customers lost billions of dollars in sales.³

(3) *Mega-risks* result from apparently known and familiar risks erupting at unprecedented scale or speed. This occurred in the escalating and cascading sequence of failures at the Fukushima electric plant in Japan (see SIDEBAR, Tokyo Electric's Fukushima Plant). The mega-risk event overwhelms the organization's capacity to manage it as a routine event. Organizations train personnel, design equipment, and establish responses for risk events up to some maximum likely scale. They judge it impractical or uneconomic to prepare in advance for larger events. The routine response to a mega-event will then be incompletely planned, and with insufficient resources and capabilities.

SIDEBAR Tokyo Electric's Fukushima Plant

The Fukushima plant was designed and constructed to cope with anticipated rare events, such as a large earthquake or a flood triggered by a tsunami. But it failed completely when the Tohoku earthquake in March 2011 generated a 14-meter high tsunami that swept over the plant's seawall, filling the basements and knocking out the emergency generators at the plant, which had already suffered severe damage from the earthquake. The plant had three nuclear meltdowns and three hydrogen explosions, and released radioactive contamination throughout the local region that

³ "Boeing fine-tunes software, creates safety group as it readies 737 Max for return." *Los Angeles Times* (Sep 30, 2019).

forced more than 100,000 people to evacuate from the region. During the next three years, Tokyo Electric paid out more than \$38 billion to compensate individuals and businesses for the disruption.

The Covid-19 pandemic appears to be a combination of a Black Swan event (except for countries such as Singapore, South Korea and Taiwan) and a Mega-event, whose scale overwhelmed the capabilities of many countries' public health authorities. The world was already familiar with occasional global outbreaks of corona and influenza viruses that cause acute respiratory symptoms, including H5N1 "avian" flu in 1997, SARS epidemic in 2003, and H1N1 in 2009. The novelty of the CoV-2 coronavirus, despite being a variant of the SARS virus, was its multi-day period when many infected people were both asymptomatic and highly contagious. The rapid spread of infections greatly exceeded what most countries' healthcare systems had prepared for in advance. The subsequent high loss of life and catastrophic economic damages illustrated the consequences from managing the early stages of a novel risk event with processes and responses designed for a familiar (routine) one.

Routine versus Novel risk management

Companies manage their routine risks with risk maps, such as that shown in **Figure 1**.

Likelihood	5					
	4					
	3					
	2					
	1					
		1	2	3	4	5
		Consequence				

Figure 1: Risk Map

Managers use their familiarity with routine risks to estimate, with some confidence, their probability of occurrence and their potential impact on the organization, typically on a scale from 1:5 (low to high). They devise risk mitigation actions that move risks from the red or yellow zones into the green zone.

Novel risks, in contrast, are events whose likelihood or consequences cannot be assessed either because no one has yet envisioned them, or because of high uncertainty about what their likelihood or consequences might be. Figure 2 illustrates this feature of novel risks. The axes represent the degree of *uncertainty* about likelihood and the degree of *uncertainty* about consequence. The lower left hand quadrant of Figure 2 is the domain of routine risk management where managers have relatively reliable information and past experiences about the events,

Uncertainty of frequency

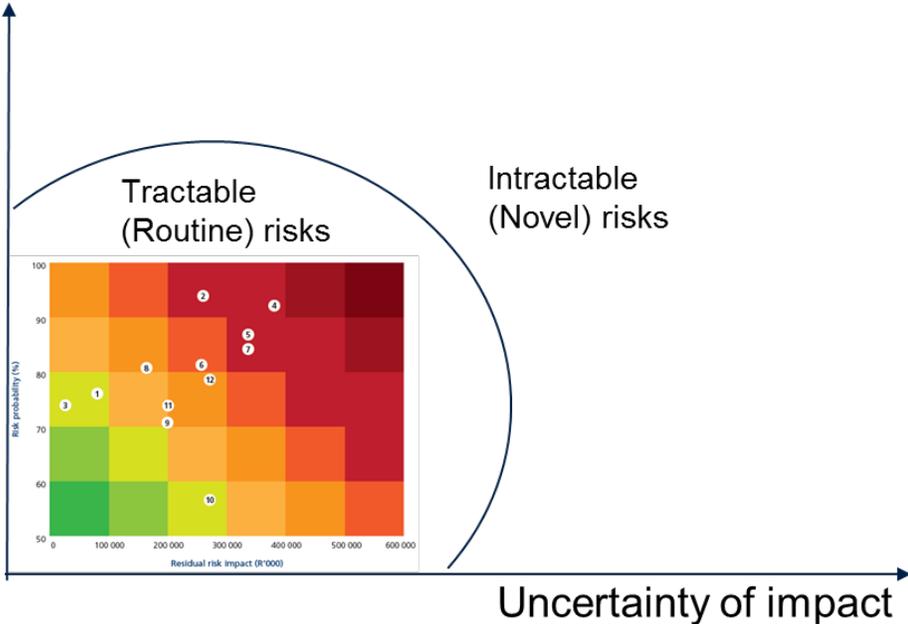


Figure 2. Routine risk management focuses on tractable risks – but do not manage novel risks

leading to low uncertainty in their estimates about likelihood and consequences. The remainder of Figure 2 is the large space of novel risks, where both the likelihood and the consequences may be difficult to quantify. These risks are largely unknown to the organization and, therefore, unanalyzed by the organization’s routine risk management processes. While ignorance about a novel risk is not a good start in managing it, problems can escalate rapidly if employees apply routine risk management to an actual novel risk. Renowned sociologist Robert Merton noted,⁴ “actions based upon training and skills which have been successfully applied in the past may

⁴ Merton, R.K., *Social Theory and Social Structure*. Free Press (1957).

result in inappropriate responses under changed conditions ... and the adoption of the wrong procedures.” The actions taken by trained employees to cope with routine risks will not just be ineffective, they can be actively dangerous, as employees believe that the risk has been mitigated while a novel risk escalates, unabated, to potentially serious, even fatal, consequences.

Routine risk management is not wrong; identifying and managing routine risks, and applying routine risk management to newly envisioned events remains essential and valuable. It is just *incomplete*. No matter how good the organization becomes in managing already-identified and newly-discovered risks, unforeseeable (or unforeseen) novel risk events will occasionally arise. They will arise less frequently if routine risk management become more effective, but they are likely to be of very high consequence when they do arise.

As another example of the failure of routine risk management in novel situations, consider the derailment of a Deutsche Bahn’s high speed ICE train, which led to 100 deaths and more than 100 serious injuries. A passenger had noticed that a large wheel had suddenly appeared and become wedged between two passenger seats. The passenger did not activate a nearby emergency brake because a prominently-displayed sign stated that travelers would be subject to a large fine if they pulled the brake without authorization, a routine risk management process to avoid unnecessary train stoppages. The passenger spent several minutes before finding a conductor to obtain authorization, but the conductor failed to reach the emergency brake before the fatal derailment occurred. After being sued by Deutsche Bahn for negligence, the conductor successfully defended his actions by claiming he followed the established rule that required him to visually inspect any problem (which in this case was several carriages away) before triggering an emergency stop. The employee’s faithful adherence to the protocol for managing a routine

operational risk delayed his response to a novel, previously unrecognized, incident of a wheel breaking loose from its axle.

Similarly, and also tragically, the loss of the *Columbia* space shuttle revealed that senior NASA personnel had failed to see the potential danger that appeared during apparently routine operations. The attempt to treat space travel as routine even extended to the project's description as a "shuttle," evoking the image of frequent, reliable flights between Boston and New York. Management's priority was to keep the "shuttle" on its schedule rather than make the special efforts that would have been required to learn more about the potential seriousness of a novel foam strike that had occurred during lift-off. The severe damage to the heat shield of the space capsule became known only after its destruction, with tragic loss of life, during re-entry into the earth's atmosphere.

Such disasters occurred in organizations that already had policies in place for identifying and assessing routine risks in their supply chains, operations, product development, and health systems. Yet these policies could not mitigate the consequences when novelty materialized during apparently routine processes. Companies need an additional set of structures and practices to *recognize* when a novel risk situation has occurred or is emerging, and to *respond* to the novel risk, in real time, under stress, and with uncertain knowledge about it.

Recognizing a Novel Risk

What does novelty look like when it appears? What is the *signature* of novelty? The best indication of the presence of novelty is that the circumstances, taken in combination, do not make sense. In routine situations, risk managers and responders quickly grasp the essential features of a familiar event, a state of knowledge referred to as situational awareness. They have

experienced the event in the past, which evolves in predictable and readily comprehensible ways, and they have been trained to manage it.

By contrast, in novel situations, responders must recognize, at the outset, that their situational awareness is low. Even when elements of the situation seem *routine*, a thoughtful observer notices novel elements or *anomalies*, things that surprise or do not make sense. For example, a senior risk manager at Boeing, with knowledge of Murphy's Law applied to complex engineering projects ("if anything can go wrong, it likely will"), could have concluded that costly problems and delays were likely to accompany the development of an entirely new plane with 1st-tier suppliers performing major tasks they had never done before, using materials never used at scale in a large aircraft, and replacing familiar analog hydraulic controls with entirely new digital ones. The Deutsche Bahn conductor could have recognized that a large, steel wheel suddenly appearing in a passenger car was not a normal, routine event, but one that foreshadowed imminent disaster, even without seeing it himself. An experienced purchasing manager for semiconductors could have recognized that soot, smoke, and large quantities of water, which accompany even a minor fire, might have compromised the integrity of ultra-clean rooms used to fabricate complex and hypersensitive microprocessors and microcontrollers. And NASA senior managers of the Columbia shuttle could reasonably have been concerned after learning that an unusually large chunk of insulation had struck the protective shielding of the re-entry vehicle during takeoff.

Individuals, however, are conditioned to recognize and respond routinely to events. They will likely see only the familiar elements that they have been trained to observe. Their operational responsibilities distract them from noticing the elements that *are* novel (see SIDEBAR Why People Fail to Recognize Novel Events).

SIDEBAR Why Do People Fail to Recognize Novel Events?

Individuals' perception of reality is often distorted because of a multitude of behavioral biases. Overconfidence and confirmation biases cause them to selectively pay attention to the data and information that confirm their experiences and initial perceptions, while the cognitive dissonance bias leads them to disregard contradictory evidence. Individuals react instinctively and quickly to situations that they believe are routine (referred to Daniel Kahneman as "System 1" thinking⁵), and grossly underestimate the range and adverse consequences of possible outcomes in the presence of high uncertainty. As they under-weight new information that is inconsistent with their prior beliefs, they accept repeated deviances and near misses as the new normal, a bias referred to as the "normalization of deviance." These biases get exacerbated by an organizational bias, group think, which causes teams to suppress and disregard inconvenient facts when assessing an uncertain situation.

Chief worry officer

Recognizing a novel risk situation requires individuals to question their assumptions and think more deeply and analytically about the situation. Such deeper, analytic thinking (called System 2 thinking, by Kahneman) is often suppressed because it is more time-consuming and psychologically and physiologically more demanding.

Consider, for example, the response of Nokia, another important customer of the Philips Albuquerque semiconductor plant where the minor, un-newsworthy fire occurred. The Nokia

⁵ Kahneman, D. *Thinking: Fast and Slow*. Farrar, Straus and Giroux (2011).

purchasing manager evaluated it, just like his Ericsson counterpart, as a routine supply chain event that did not require additional thought or effort on his part. But Nokia required that information about any anomalous or unusual event, anywhere in Nokia's extensive supply chains, should be reported to Perri Korhonen, a senior vice president with few specific operational responsibilities. His full-time job was to be a top troubleshooter, or – as we have come to describe the position – the “chief worry officer.” The Nokia philosophy was, “We encourage bad news to travel fast. We don't want to hide problems.” With time to think deeply about the supplier's fire, Korhonen placed the affected parts on a special watch list, explored alternative sources of supply, and concluded that parts shortages from the Albuquerque plant could disrupt more than 5% of the company's annual production.

Korhonen mobilized a 30 person multi-function team to manage the threat. Engineers redesigned some of the chips so they could be sourced from alternative suppliers, and the team accelerated the purchase of most of the remaining chips from other plants, but still had two types of chips for which Philips was the only supplier. Korhonen called his CEO, reaching him on the corporate plane, briefed him about the situation, and had the plane rerouted to land at Philips headquarters in The Netherlands so the CEO could meet with his Philips counterpart. The two CEOs announced, after the meeting, that “Philips and Nokia would operate as one company regarding those components.” In effect, Nokia could use Philips as its captive supplier for the two scarce chips. The relationship enabled Nokia to maintain production of existing phones and launch its next generation of phones on time while a major competitor, Ericsson, exited the mobile phone market.

This classic case study highlights that a formal risk management system that focuses only on routine risks can breed complacency. Identifying novel risks requires paranoia, the opposite of

complacency. Korhonen's job at Nokia was to be continuously paranoid about what could go wrong in the supply chain. He had the time to monitor and analyze emerging risks, and the authority to take creative, novel actions in real time. As a postscript to this story, while Nokia had an excellent structure to identify and manage novel risks in its supply chain, it did not have a comparable structure for anticipating novel disruptions to its strategy, leading to massive losses of market share and income when a computer manufacturer, Apple, introduced the iPhone into the mobile phone market.

Swissgrid⁶, the nation's electricity transmission system operator, has established three processes to identify emerging risks. When the senior risk officer becomes aware of a potential novel risk event, he schedules an "Extraordinary Risk Workshop" to raise the question "could this happen here?" Examples of such events included the first instance of a cyber-attack, a major change in European Union electricity market regulations, and an unexpected large-firm bankruptcy in the country. Senior managers and risk officer from every business unit attend the extraordinary risk workshop, along with subject matter experts about the novel event. After deliberation, the group creates an action plan that the risk officer brings to the leadership team at an "Extraordinary Executive Risk Workshop" for approval and implementation.

Swissgrid also installed a user-friendly app, RiskTalk, on employees' mobile phones for them to quickly and conveniently report on routine risks related to safety violations, maintenance problems, and imminent equipment failures.⁷ A report, however, could also be an indicator of a

⁶ Kaplan RS and Mikes, A, "Swissgrid: Enterprise Risk Management in a Digital Age," Harvard Business School Case 119-045 (November 2018).

⁷ Mikes, A. "RiskTalk: Can a Better Conversation Help Fend Off Disaster?," *RiskNet* (27 October 2017).

novel situation. A rotating cadre of risk, safety, and quality managers monitored the app's messages in a central control room. The attending manager, like Nokia's Korhonen, could conduct a more time-consuming analysis, even when an event's description appeared to be routine, to determine whether to activate a non-routine response. By reviewing multiple reports coming in from the field, risk managers connect the dots among apparently small and unconnected reports to identify an emerging novel event. In effect, the triage team serves as the company's chief worry officers, empowered to think more deeply about and respond quickly to a potentially novel risk event.

For potential external novel risks, a senior crisis manager led the development of a real-time national crisis management platform accessed by the company, the Swiss army, Swiss national police force, and several other federal and state (canton) agencies and corporations. Each entity uses the platform to report any issue it learns about, such as a forest fire, an accident triggering a massive traffic jam, or unusual snow conditions or avalanches in the Alps. Swissgrid risk managers, connected to the platform, get early visibility into external risks that, if left unaddressed, could lead to novel situations that would interrupt the reliable flow of electricity to national and European power grids. The Swissgrid CEO noted "Our business, with individual risks and intricate connections spread across all our units, is too complex for any one individual to fathom. Yet we cannot wait for problems to show up and then solve them like firefighters. [The systems we have put in place] enable us to solve a lot of problems proactively." The three processes enabled the company to anticipate many novel risks and transform them into routine ones that could be mitigated and managed in advance.

Responding to a Novel Risk Event

Responses to a routine risk event involve pre-programmed and well-rehearsed actions:

1. Recognize the situation
2. Recall the script, the game plan, for this situation
3. Mobilize trained employees to execute the pre-determined game plan, with minor customization for any uniqueness in this specific situation.

The sequence enables swift, decisive, effective action for events within the domain of the organization's routine understanding and experience. But such a response is a grave weakness and vulnerability when the risk is novel. The "right-of-boom" response to a novel risk event must be completely different. By definition, the organization does not have an existing script or playbook to roll out to mitigate the event, and nothing in an operating or risk manager's background enables them to respond automatically and quickly to the boom. Leaders in the immediate post-boom setting must resist the temptation to take immediate decisive action unless an instantaneous action is required to avoid imminent danger, such as the situation with the Deutsche Bahn dislodged wheel.

Managers responding to a novel situation, must be humble, recognizing that they do not fully understand the situation, the situation will likely continue to change, and it will take time to learn about and develop good solutions. The company needs a good enough decision, soon enough to matter, communicated well enough to be understood, and carried out well enough to work – until a better option emerges from learning by doing.⁸ Companies can achieve these objectives by deploying (1) a critical incident management team, (2) staffed with the right people, who (3) engage in an iterative and agile problem-solving process. We discuss each in turn.

1. *Critical Incident Management Team (CIMT)*

⁸ Leonard, H.A., et al. Something Old, Something New: Army Leader Development in a Dynamic Environment. RAND Report MG-281 (2006).

The critical incident management team (CIMT), a term originating in public sector crisis management, oversees all aspects and responses to the event. The CIMT must decipher the situation, identify the critical issues faced by the company, and establish the priorities among the firm's multiple, and now competing, constituencies and interests when deciding on the actions to take. The CIMT can delegate the answers to specific questions to other individuals or sub-groups but it must maintain responsibility for coordinating all aspects of the response.

The CIMT should meet at least daily, and more often if the event is evolving rapidly. The team manages the communication within the firm and coaches the CEO on external communications. We recommend that both internal and external communications follow three guidelines: be brutally honest about the reality of the situation, including what is not known; provide a rational basis for hope; and be empathetic to the concerns of all stakeholders affected by the event.⁹

2. Recruit the right people for the CIMT

The CIMT should include people who have expertise about the novel risk event. For example, a novel disruption of a company's supply chain will require people from operations, product design and engineering, logistics, and marketing. For a novel medical event, such as the Covid-19 epidemic, the team needs medical, public health, and public policy expertise, which could be obtained by including members from outside the firm. For managing the delays in large-scale product development, such as a new Boeing aircraft, the CIMT should include representatives from suppliers. Since decisions will be made that affect all the firm's stakeholders, the CIMT must include members who understand the firm's priorities, values, and constituencies.

⁹ The first two of these principles were articulated by Admiral James Stockdale in Jim Collins' book, *Good to Great*. Stockdale, the senior American officer incarcerated in the North Vietnamese POW camps, has been credited with saving the lives of many fellow inmates.

The CIMT will consist of individuals at different levels of the company's hierarchy, with diverse sets of skills, organized in a flat structure, and with the authority to commit organizational resources in a process of experimentation and rapid iteration. The membership on the team may also change over time as events unfold and the situation changes.

3. Use an Agile Problem-Solving Method

The CIMT needs to follow a disciplined, iterative, and agile problem-solving approach. The team should first affirm the core values that must be preserved and that will underlie and guide all its decisions. The core values anchor the difficult decisions that lie ahead. At a time of crisis, not all decisions will turn out to be correct, and not all constituencies' needs will be met. But by anchoring on trying to do the right thing for those who matter the most, the CIMT will be able to do the best that it can, and know afterwards that it was the best it could have done at the time.

With the core value established, the CIMT begins an agile problem solving approach, which follows the logic of the OODA loop – Observe, Orient, Decide, Act – devised by the Korean Conflict-era pilot, Air Force Colonel John Boyd. The OODA loop emphasizes shortening the length of time between the occurrence of a stimulus and the activation of the response to it.

Boyd's goal in aerial combat was to have a faster OODA loop than his adversary, so that he was driving the evolution of the event. In a crisis situation, the CIMT's OODA loop must be faster than the speed of events following the novel risk event. The team first observes by becoming aware of the situation. It then gets oriented, making sense of what was observed, the key elements of the situation. Then it decides by formulating various options, working out the consequences of each option, and selecting the best one, guided by the core values. Finally, the team acts to implement the chosen option – treating its approach not as a permanent commitment to a course of action, but as an ongoing experiment.

All decision made by the CIMT are tentative as it strives to be “probably approximately correct” with the limited information available in the volatile, uncertain, and dynamic post-boom environment. Being “perfectly exactly correct”¹⁰ cannot be its standard for performance. The CIMT will, in hindsight, have made some incorrect assessments and decisions, but it has no alternative other than to learn from its prior decisions and actions, acquire new information from the event, and act again, and again to stay ahead of unfolding events.

The dynamics of CIMT discussions are also important. We recommend that someone other than the CIMT head facilitate the discussion. This enables the senior person to devote full time to listen and to process the information. By listening, rather than speaking, the CIMT head also reduces the chances for group think, where subordinates defer to what they perceive the chief decision-maker may already have decided. The CIMT, as already noted, will bring together a diverse group of people, many of whom may never have met before. Some could fear to speak out candidly and honestly among unfamiliar people, especially if junior to many of them. Alfred Sloan, founding CEO and Chairman of General Motors, would ask his leadership team what could go wrong with an action about to be taken. If no one dissented, he dismissed the meeting and said discussion would resume the next day when people had taken more time to think about the pitfalls. The CIMT discussion leader has to encourage inquiry, not advocacy, for team members to work collectively and productively to find the best near-term decisions and solutions. The meetings need to be psychologically safe for individuals to offer untested ideas and to dissent and disagree. What is right is far more important than who is right.

¹⁰ Leslie Valiant, *Probably Approximately Correct*, Basic Books, New York, NY 2013.

Responding to the emergence of the Covid-19 epidemic, Singapore, Taiwan, and South Korea activated incident management teams. Singapore established its team after the SARS pandemic in 2003. It gained real-time experience, during the subsequent H1N1 and MERS outbreaks,¹¹ and used simulated epidemic scenarios to practice between actual outbreaks. When the novel COV-2 virus emerged in early January 2020, the three countries recognized the threat, and mobilized their teams. They immediately activated large-scale testing, contact tracing, and selective isolation and quarantine. These early actions enabled schools, businesses and other enterprises to keep functioning while the countries experienced among the world's lowest incidence of cases and deaths per 1 million residents.¹² What was a novel event to the rest of the world, was a routine risk management exercise for the three countries. But despite extensive practice and early action, the Singapore team's response was not perfect. It allowed migrant workers to travel into the country where they soon infected existing workers living in high-density housing. A second wave of infection and contagion broke out that required large-scale shutdowns and physical isolation across the island nation.

Some novel risks do not allow for the luxury of a central critical incident team. Time could be of the essence and details about the situation may be difficult to communicate to company headquarters from the location where the event occurred. In these situations, critical responses must be delegated to personnel closest to the event as described in the Sidebar, Adventure Travel Agency.

¹¹ Hille, K. and White, E. Containing Coronavirus: Lessons from Asia. *Financial Times* (16 March 2020).

¹² Hsu, L.Y and Tan, M. What Singapore can teach the U.S. about responding to Covid-19. *STATNews.com* (23 March 2020).

Sidebar: Adventure Travel Agency

A Boston-based travel agency offered “off-the-beaten-path trips” to experienced, mature travelers. It initially employed US tour guides who were familiar with the agency’s targeted clientele. But the CEO soon learned, painfully, that the any given trip could have accidents and illness among its mature client base, and disruptions from extreme weather, natural disasters, local political unrest, hotel cancellations, and airline delays, strikes, and accidents. For this company, novel risks came with its territory.

The company executed a lengthy, costly process to replace its experienced cadre of American guides with local-country guides who had considerable knowledge of their region and people. It empowered the local guides to problem-solve and implement the response to any novel situations that arose during a trip. The company believed that the guides had (a) the best information about the situation and the challenges that had arisen, (b) the best knowledge, especially when combined with connections to local people and resources, to develop creative response options to the novel event; (c) the best understanding of the preferences of the tour group among the various identified responses; and (d) the ability to put the chosen solution quickly into practice.

The company’s headquarters remained available for actions best done by a centralized staff such as to re-schedule flights or make new hotel reservations. But the guides had the responsibility to follow the OODA loop process, “*Act early. Act aggressively. Act often. Make mistakes. Reassess. Reassess. Reassess.*” with a bias to keep travelling as long as that remained the preference of the travelers.

The travel company’s decentralized risk management process violates established standards and protocols for routine risk management since it empowers operations people to also serve as risk managers. But independent and centralized routine risk management can be too distant and too delayed to respond to novel events. It would have only limited information about the situation faced by the local tour, would not be aware of the local options available, and would have little-

to-no capability to implement a local response. It provides another example of how responses to novel events must depart from the established practices for managing routine risks.

Conclusion

Risks come in many forms and flavors. Companies can manage the risks that they know about and anticipate. But novel risks, those unanticipated, those arising from complex combination of seemingly routine events, and those occurring at unprecedented scale and magnitude, can still arise. Companies need to detect the arrival of such novel risks, and then activate a response very different from its normal risk management of routine risk events. The response must be rapid, improvisational, iterative, and humble since not every action taken will work as intended.

Responding, post-boom, to novel events requires continual trial and error by a dedicated crisis management team whose actions will eventually mitigate the worst consequences from the adverse event.