Novel Risks

Robert S. Kaplan
Dutch Leonard
Anette Mikes
Novel Risks

Robert S. Kaplan
Harvard Business School

Dutch Leonard
Harvard Business School, Harvard Kennedy School

Anette Mikes
Oxford University

Working Paper 20-094
Novel Risks
Robert S. Kaplan¹, Dutch Leonard², and Anette Mikes³

Abstract
All organizations now practice some form of risk management to identify and assess routine risks for compliance; in their operations, supply chains, and strategy; and from envisioned external events. These risk management policies, however, fail when employees do not recognize the potential for novel risks to occur during apparently routine operations. Novel risks — arising from circumstances that haven’t been thought of or seen before - make routine risk management ineffective, and, more seriously, delude management into thinking that risks have been mitigated when, in fact, novel risks can escalate to serious if not fatal consequences. The paper discusses why well-known behavioral and organizational biases cause novel risks to go unrecognized and unmitigated. Based on best practices in several organizations, the paper describes the processes that private and public entities can institute to identify and manage novel risks. These risks require organizations to launch adaptive and nimble responses to avoid being trapped in routines that are inadequate or even counterproductive when novel circumstances arise.

¹ Harvard Business School
² Harvard Business School and Harvard Kennedy School
³ Saïd Business School, Oxford University
Novel Risks

All organizations practice risk management. Yet consider the following events that slipped through their company’s risk management systems.

Boeing started the new century with the development of an entirely new aircraft, the 787 Dreamliner, which it expected would start commercial flights in May 2008. Boeing had extensive experience over more than a half century of designing and building advanced aircraft, and presumably knew the potential risks associated with new product development. But the company 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. Not to allow the 787 development project be an unusual event, Boeing’s next plane launch, the 737MAX, had 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.

On June 3, 1998, Deutsche Bahn’s high speed ICE train derailed, causing a deadly crash that killed 101 passengers and left more than a hundred other people injured. A passenger had noticed a faulty wheel that had become wedged between
two passenger seats. The passenger did not activate a nearby emergency brake because a prominently-displayed sign warned passengers that pulling the brake without authorization would lead to a large fine. The passenger spent several minutes searching for and finally finding a conductor to obtain authorization, but neither had the time 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 and trained routine that required him to visually inspect any problem, which in this case was several carriages away, before triggering an emergency stop.

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 notified the purchasing managers of all the plants’ customers about the fire, reporting superficial damage had occurred, including destruction of the small quantity of 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 delay.

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 the 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.

These disasters shared a common feature. They occurred when each organization had well-established policies for identifying and assessing routine risks, whether they arose in product development, safety, or supply chains. Yet the policies failed when employees failed to recognize the potential for new or novel risks to materialize during apparently routine processes. Such novel risks make routine risk management ineffective, and, even more serious, delude management into thinking that risks have been mitigated when, in fact, the novel risks are escalating to serious if not fatal consequences.

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 The novelty of the situation included risks that Boeing had never encountered before: new structural materials, composites rather than aluminum for the airframe; a complex global supply chain that required first-tier suppliers to take on unprecedented responsibility for design, engineering, and integration; and electronic controls, with large, lithium batteries for backup, to replace the hydraulic controls used in previous generations of aircraft. 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.”

Novelty was also present in the design of the 737MAX when engineers introduced a larger, much 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 at least a couple of cases, however, the novel situation of losing tactile control over the aircraft, while alarms were flashing and warning bells were sounding in the cockpit, immobilized the anticipated responses of otherwise competent and experienced pilots.

Sources of novel risks

A previous paper (Kaplan-Mikes, 2012) described how to design enterprise risk management systems to identify, assess and mitigate routine risks (see Figure 1). The term “routine” does not imply that these risks are unimportant, easy to handle, or not dangerous. Their “routineness” comes from managers’ familiarity with them, enabling them to mitigate or prepare for them in advance with situation-specific approaches. For example, following the taxonomy in Figure 1, companies reduce routine operational

---

risks, including employee misbehavior and violation of standard operating procedures by frequent communications about mission and values, deployment of internal controls, corporate compliance and enforcement processes, extensive employee training on standard operating procedures, vigorous elimination of hazardous and unsafe conditions, and strong, independent internal and external auditing reviews. For strategy risks, companies conduct frequent risk review meetings to identify, assess, mitigate, and manage the known risks associated with their strategies. They identify the existence and impact of external risks through war gaming, stress tests, scenario planning, and continual external scans. Once identified and assessed, companies reduce the impact of external risks through redundancy, insurance, hedging, and training and contingency planning for how to react should an external risk materialize.
### Three Categories of Risks and their Risk Management Tools

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Controllability and Relationship to Strategy</th>
<th>Control Approaches</th>
</tr>
</thead>
</table>
| I. Operational and Compliance | Organizations can prevent or cost-efficiently minimize occurrence of risk. There is no strategic benefit from taking these risks. | Internal control  
Boundary systems  
Mission and value statements  
Internal audit                                                                                                                                                                                                   |
| II. Strategy execution        | Taking these risks is essential for achieving strategic returns. Organizations may reduce the likelihood and impact in cost-efficient ways. | Risk identification with key risk indicators and highly-interactive risk workshops  
Quantify with risk (heat) maps  
Risk mitigation initiatives and risk owners  
Resources allocated to fund the risk mitigation initiatives                                                                                                                                               |
| III. External                 | Organizations cannot control the occurrence of such risks, but may be able to prepare and thus reduce their impact. | Risk “envisionment” via scenarios and war games  
Contingency planning  
Insurance and hedging programs                                                                                                                                                                                |

**Figure 1: Three Categories of Risks**

Source: Adapted from Kaplan-Mikes (2012)
Such management of routine, anticipated risks, however excellent and worth doing, does not work and, even worse, may delay the response to a novel operational risk incident, as occurred on the Deutsch Bahn train with the runaway wheel. The tragic loss of the space shuttle Columbia revealed that even an organization (NASA) with superbly educated and trained personnel failed to see the novelty and potential danger during apparently routine operations, especially when senior management’s priority was to keep the mission on schedule rather than take time to learn more about a potential safety issue.

Operational failures have also occurred when rogue traders in financial services firms exploited previously unrecognized gaps in financial and internal control systems, and warning signals of such breaches were ignored by supervisors and internal auditors. Hostile external agents have launched novel cyber-attacks through an unprotected supplier’s system to capture highly sensitive information from a company’s IT system (the experiences of Target Corporation and Equifax, among many others), or cause the company’s global IT systems to crash completely, as happened to Maersk.

Novelty can arise from a familiar risk that occurs at an unprecedented scale and overwhelms operators, such as the loss of manual control over an aircraft. Novel risks can also arise from increased complexity and the confluence of multiple forces, that may be familiar and manageable in isolation, but in combination cause unique challenges. This occurred in the escalating and cascading sequence of failures at the Three Mile Island nuclear plant, and at the Fukushima electric plant in Japan. 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. It failed when both events occurred at the same time.
Identifying and managing routine risks remains essential and valuable. Routine risk management is not wrong; it is just incomplete. A truly effective and comprehensive risk management approach must also grapple successfully with novel risks.

Risk management for novel events requires two distinct mechanisms. First, the organization must recognize when a risk situation is, in fact, novel. Second, it must develop a process to deal with the identified novel risk. By definition, the organization will not have an existing script or playbook to roll out to mitigate an emerging novel risk. It must, therefore, activate a mechanism that can learn about the novel risk, develop a tentative approach to deal with it, and then implement the response, perhaps repeating the identification, planning, and implementation steps multiple times as it learns by doing.

We describe the two novel risk mechanisms below.

**Recognizing a Novel Risk**

How does novelty generally present itself? What is its “signature” that observers can look for? The best indication of novelty is that elements of the circumstances do not make sense. In routine situations, risk managers and responders can grasp the essential features of the situation, a state of understanding often referred to as situational awareness. They observe data and key indicators that, collectively, make sense. The event is familiar and well-understood, and evolves in predictable and readily comprehensible ways.

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, novel elements or anomalies, appear; things occur that are surprising or that 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 reasoned, how likely is it that developing a new plane with 1st-tier suppliers performing major tasks they had never done before, fabricating a large aircraft with materials never used at scale before, and replacing analog hydraulic controls used for decades, with electronic ones, would not encounter major costly problems and delays along the way? The Deutsche Bahn conductor could have recognized that a large, steel wheel suddenly appearing in a passenger car was not a normal, routine event. A purchasing manager for semiconductors might reasonably have concluded that the soot, smoke, and large quantities of water that accompany even a minor fire might have compromised the integrity of clean rooms used to fabricate complex and hypersensitive microprocessors and microcontrollers. And NASA senior managers of the Columbia shuttle could reasonably have been concerned when the protective shielding of the re-entry vehicle could have been damaged during takeoff.

Individuals, however, who are conditioned, if not highly tuned to recognize and respond to routine events, will likely see only the elements that are familiar, and, distracted by their operational responsibilities, fail to notice the elements that are novel. They fall victim to a multitude of behavioral biases; their 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. The failure to recognize novelty in a situation has been described as “System 1” thinking in which individuals react instinctively and quickly to situations that they believe are routine. By acting too quickly, they grossly underestimate

---

the range and adverse consequences of possible outcomes from risky situations. As they under-weight new information that is inconsistent with their prior beliefs, they accept deviances and near misses as the new normal, a bias referred to as the “normalization of deviance.” These biases get exacerbated by group think, which causes teams to suppress and disregard inconvenient facts about the novelty of the situation.

Recognizing a novel risk situation requires Kahneman’s “System 2” thinking in which individuals question their assumptions and think more deeply and analytically about the situation. System 2 thinking 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 that experienced the minor, un-newsworthy fire. The Nokia purchasing manager, also informed about the event, evaluated it, just like his Ericsson counterpart, as a routine supply chain event that did not require additional thought or effort on his part (a System 1 analysis). But Nokia had established a procedure that any information about any anomalous or unusual event, anywhere in Nokia’s extensive supply chains, should be reported to Perri Korhonen, senior vice president of operations, logistics and sourcing. Korhonen had no operational responsibilities; his full-time job was to be a top troubleshooter. His philosophy was, “We encourage bad news to travel fast. We don’t want to hide problems.” After hearing about and thinking more deeply about the fire at a key supplier’s plant, Korhonen placed the affected parts on a special watch list and offered to send engineers to Albuquerque to help restore the plant to full-scale operations. The Albuquerque plant manager naturally refused, believing he had the situation fully under control and did not require engineering
assistance from Finland (again a deployment of System 1 routine risk analysis). But
Korhonen persisted in his analysis and learned that shortages of components from the
Albuquerque plant could disrupt more than 5% of the company’s annual production.

Korhonen, at this point, recognized the fire had become an emerging novel risk. He
activated an extensive response by assembling 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 accelerated the purchase of most of the remaining chips that
were available from other plants. But Nokia remained vulnerable for two types of chips
for which Philips was the only supplier. Korhonen called his CEO and reached him on
the corporate plane. After briefing him about the situation, the CEO rerouted the plane to
land at Philips headquarters in Eindhoven, Netherlands so he could meet with his Philips
counterpart. The meeting ended with a joint statement that “Philips and Nokia would
operate as one company regarding those components.” In effect, Philips had become the
captive supplier to Nokia for the two scarce chips. Nokia was then able to maintain
production of its existing phones and launch its next generation of phones on time while
one of its largest competitors exited the market.

This classic case study highlights that a formal risk management system that focuses only
on routine risks can breed complacency. The opposite of complacency is paranoia, as
noted by former Intel CEO Andrew Grove, when writing his history at the company,
“Only the Paranoid Survive.” Korhonen’s job at Nokia was to be continuously paranoid
about what could go wrong in Nokia’s supply chain. He served as the company’s “chief
worry officer” (our colloquial term for his role). 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 failed to create a comparable structure for responding to novel disruptions to its strategy. In 2007, it fell victim to Apple’s unexpected entry, with the iPhone, into the mobile phone market.

While many novel risks emerge rapidly, others emerge gradually out of more ordinary circumstances. They appear to be routine at first, but along the way they morph into novelty. Swissgrid⁵, its country’s electricity transmission system operator, dealt with this problem with two mechanisms. First, it developed a user-friendly app that it installed on employees’ mobile phones. Employees could now quickly and conveniently report on anomalies and unusual patterns of activity they saw in the work environment. Many of the reported anomalies helped Swissgrid manage routine risks such as equipment failures and safety violations. A report, however, could be an indicator of a novel situation. The company did not require employees to classify the report as either routine or novel. Its risk managers reviewed each report and developed an appropriate response. The risk manager could decide to conduct a more time-consuming analysis, even when an event’s initial description appeared routine, to determine whether to activate a non-routine response. By reviewing multiple reports coming in from the field, risk managers could connect the dots among apparently small and unconnected reports to identify an emerging novel event. In effect, the company’s risk managers served also as its chief worry officers, empowered to do deeper System 2 thinking before responding to an event.

Deploying a risk communications app to the front lines expanded the number of people

communicating timely information about anomalies and pattern-breaks that would be the early signals of a potentially novel risk event.

A senior Swissgrid crisis manager also led the development of a real-time national crisis management platform accessed by the company, the Swiss army, several other large companies, and all federal and state (canton) agencies. Each company and agency used the platform to report any external issue that it was seeing or experiencing, such as forest fires, declining water levels on the Rhine River, an accident triggering a massive traffic jam, or unusual snow conditions or avalanches in the Alps. Swissgrid risk managers were connected to the platform, giving them 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. As the Swissgrid CEO noted (Kaplan-Mikes, 2018), “Our business, with individual risks and intricate connections spread across all our units, is too complex for any one individual to fathom. Yet we can’t 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.”

**Responding to Novel Risk Event**

Enterprise risk management systems identify and manage routine risks in a cost-effective way. Risk managers ensure that standard responses are in place to treat the wide variety of known risks that may arise. The risk management function develops practices and expert teams to apply them, and provide the training, equipment and leadership for pre-programmed rules, procedures and actions in response to the known risks. The sequence is:
1. Recognize the situation
2. Recall the script, the game plan, for this situation
3. Mobilize your training to execute the pre-determined game plan, with minor customization for any uniqueness in this specific situation.

The sequence, when applied to a well-defined list of risks, with early warning indicators and accountability structures, allows traditional risk management to become routinized and implemented. It works well when the presenting risk is within the organization’s prior experience and is, indeed, routine. But it is a grave weakness and vulnerability when the risk is novel. Missing from the enterprise risk management repertoire are the processes, mechanisms, tools, training, and actions to be followed when confronted with a novel and escalating risk.

Sociologist Robert Merton warned, “actions based upon training and skills which have been successfully applied in the past may result in inappropriate responses under changed conditions ... and the adoption of the wrong procedures.” When the environment changes, rules that worked well in normal, routine situations can aggravate or even cause a disaster in novel situations, certainly the situation that occurred at the Three Mile Island nuclear plant in 1979. Executives often describe such invalid actions as “operator error,” a catch-all category to disguise how the company’s training actually led to the risk management failures since no one recognized that the routine responses were pre-destined to fail when applied to novel risks.

Responding to novel risks requires a different sequence of actions:

1. Recognize that the situation is not routine and that existing scripts, templates or game plans should not be used in this situation.
2. Formulate a new approach

---


3. **IMPROVISE!** Execute a response that is, at best, unpracticed and, at worst, requires violating normal rules, procedures, and norms established for routine situations.

Managing novel risk situations often requires rapid innovation, under urgent and stressful conditions, including the presence of fear. Based on learned practices in crisis management, the responses to novel risks requires organizational agility with creative and effective problem solving. The response is best crafted by small teams with a diverse collection of skills organized in a relatively flat structure and with the authority to commit organizational resources in what is understood to be a process of experimentation and rapid iteration, combined with a high tolerance for results that may initially be disappointing until better ideas get developed. Teams decide the data they need while remaining open to the possibility that something important might still be missing. Authoritative centralized response must be deferred to later, after the new course of action has been developed; for example Korhonen did not inform or mobilize his CEO until the situation had been diagnosed and decisions made. He reached out to the CEO when he needed his authority to negotiate the temporary “we’re one company” arrangement with Philips.

Reverting back to the Boeing experience of a continual sequence of unexpected and costly delays during the 787 Dreamliner development project, consider the alternative approach used by Jet Propulsion Laboratory, a NASA systems integration contractor, for its projects for unmanned missions to Mars. Recognizing the novelty in any new mission, JPL required that the mission have both budgetary and time reserves to deal with emerging, difficult problems that arose unexpectedly during the 5 year development

---

7 Kaplan RS and Mikes A “Jet Propulsion Laboratory,” Harvard Business School Case 110-031 (February 2010).
period. When the best efforts of internal engineering staff could not solve a problem, they had the option to create a “tiger team” of internal and external experts to focus on the issue. This enabled the problem to become visible and solvable within the time and budget constraints of the project, as evidenced by the sequence of highly-successful Mars mission since the risk management protocol was established.

An example of extreme decentralization to respond to novel events was implemented by a Boston-based travel agency that offered “off-the-beaten-path trips” to experienced, mature travelers. Initially, the agency used young and athletic US individuals as tour guides since these people, based on close association with their older relatives, neighbors, and teachers, were familiar with the agency’s targeted clientele. The company did extensive and detailed planning for each trip so that it could deliver amazing adventure and unusual local experiences to its targeted clientele. But the CEO soon learned, painfully, that the adventure trips experienced novelty from accidents and illness among its mature client base, extreme weather, political unrest, local insurrections, terrorist attacks, hotel and travel cancellations, local strikes of transportation and hospitality personnel, earthquakes, floods, airline delays, and even, tragically, airline and transportation accidents. For this company, novel risks came with its territory.

The company executed a lengthy, costly process to replace its existing and experienced cadre of American guides with local-country guides who had considerable knowledge of the region and its people. It empowered the local guides to problem-solve and implement the response to any novel situation 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 role for the company’s headquarters was to train and educate the guides with the principles and values that should guide any response. Guides could seek assistance from Boston for actions best done by a centralized staff with ready access to computers and high-speed Internet, such as to re-schedule flights or make new hotel reservations for everyone in a group. But the guides were told they had the responsibility to create a plan, and then “Act early. Act aggressively. Act often. Make mistakes. Reassess. Reassess. Reassess.” The bias was to keep travelling as long as that remained the preference of the travelers.

The travel company’s approach for decentralized risk management by local operational people contradicts traditional risk management standards and protocols to have risk management based in a separate location and act independently from line operations. Such an approach would, of course, not work to identify and mitigate the novel risks inherent in the travel company’s setting and strategy. Centralized risk management would be too distant and too delayed from the situation where the risk had materialized, would have had limited information about the situation faced by the local tour, not been aware of the local options available, and no capability for implementing a local and novel response.

Swissgrid introduced its own processes for decision making about novel risks. Its regular enterprise risk management system included regular risk workshops for each organizational unit, including the executive office and the board, to identify known risks,
assess their likelihood and magnitude, set priorities for mitigation, allocate resources for risk mitigation initiatives, and provide regular feedback on the results. Occasionally, however, a novel risk event emerged in the environment raising the question “could this happen here?” Examples included the first instance of a cyber-attack, a major change in European Union electricity market regulations, an unexpected bankruptcy that disturbed a stable-looking ecosystem elsewhere in Switzerland, or a major decline in the navigability of the Rhine River. Rather than wait for the next scheduled executive risk workshop, the senior risk officer scheduled an “Extraordinary Risk Workshop” for any new or emerging risk. Senior managers from every business unit with their unit’s risk officer attended along with subject matter experts relevant to the novel risk. The group created an action plan that was brought to the leadership team at an “Extraordinary Executive Risk Workshop” for approval and implementation. In this way, the company strove to anticipate and mitigate in advance its novel risks.

The ability to routinize risk management is an enormous organizational strength that permits risk managers, through experience and advance planning, to deal quickly and effectively with a host of risks. Moreover, the ability to look ahead – to imagine alternative futures and risks – and make effective plans, and train employees in advance of these occurrences can transform potential losses and disasters into manageable, routinely handled events. Preparation now underway in many companies for the anticipated physical and systemic impact of climate risk can be thought of in this vein.

At time of writing, the emergence and impact of the new Covid-19 virus reminds us again about the inescapability of novel risks. Such risks require adaptive and nimble responses that allow for flexibility and creativity. Unless risk managers can improvise effectively
and operate flexibly, they (and their organizations) will be trapped in routines than can prove inadequate or even counterproductive. And unless companies develop in advance the teams, processes, and capabilities to recognize and address novel circumstances, they have left their stakeholders vulnerable to all of the things they haven’t seen before or thought of yet.