



Organizational disasters: why they happen and how they may be prevented

Chun Wei Choo

University of Toronto, Toronto, Canada

Abstract

Purpose – The purpose of this paper is to look at why organizational disasters happen, and to discuss how organizations can improve their ability to recognize and respond to warning events and conditions before they tailspin into catastrophe.

Design/methodology/approach – A review of research on organizational disasters suggests that there are a number of information difficulties that can prevent organizations from noticing and acting on warning signals. The paper describes these difficulties using recent examples of organizational mishaps from: 9/11, Enron, Merck Vioxx withdrawal, Barings Bank collapse, *Columbia* Space Shuttle breakup, and Children's Hospital Boston.

Findings – The paper identifies three types of information impairments that could lead to organizational disasters: epistemic blind spots, risk denial, and structural impediment. It examines common information and decision practices that make it hard for organizations to see and deal with warning signals. Finally, the paper suggests what individuals, groups, and organizations can do to raise their information vigilance.

Originality/value – The paper shows that organizational disasters have a structure and dynamic that can be understood, and proposes a number of strategies by which organizations can become better prepared to recognize and contain errors so as to avert disaster.

Keywords Disasters, Management failures, Information management, Decision making

Paper type Conceptual paper

1. Introduction

When we think of major organizational disasters like a corporate collapse or a chemical plant accident, we tend to make two assumptions: that the failure was caused by human error or machine malfunction; and that the failure happened suddenly with little or no prior warning. In fact, research into organizational disasters suggests that both assumptions are incorrect or at least incomplete. While human or machine error may be the event that precipitates a disaster, such error lies at the end of a chain of other causal factors. Moreover, most organizational disasters incubate over long gestation periods during which errors and warning events accumulate. While these warning signals become painfully clear in hindsight, why is it so hard for organizations to detect, recognize and act on these precursor conditions before they tailspin into tragedy? This paper suggests that warning signals are not recognized and acted on because of information impairments that cause organizations to disregard warning signals so that incipient errors and problems are allowed to escalate, leading eventually to large-scale breakdown. We identify three types of information impairments derived from theoretical research and case analyses of organizational disasters: epistemic blind spots, risk denial, and structural impediment.



As a result of these information difficulties, warning signals that emerge during the disaster incubation period are filtered out or not recognized as such. Because warnings are not acted on, problems build up and intensify, causing the organization to finally lapse into systemic failure (Figure 1).

In the following sections, we look at why disasters happen, examine the three types of information impairments, and discuss what organizations can do to reduce the risk of catastrophic breakdown.

2. Why disasters happen – theories of organizational disasters

Organizational failures always have multiple causes, and focusing only on human error misses the systemic contexts in which the accident occurred and can happen again in the future. Reason (1997) sees human error as "active failures" that are committed at the "sharp end" of the system by individuals. These errors are more a consequence than a principal cause of the accident. They occur because of "latent conditions" that are an inevitable part of organizational life:

Latent conditions are to organizations what resident pathogens are to the human body. Like pathogens, latent conditions – such as poor design, gaps in supervision, undetected manufacturing defects or failures, unworkable procedures, clumsy automation, shortfalls in training, less than adequate tools or equipment – may be present for many years before they combine with local circumstances and active failures to penetrate the system's many layers of defenses (Reason, 1997, p. 10).

Perrow's (1999) Normal Accident Theory maintains that major accidents are inevitable in interactively complex, tightly coupled technological systems, such as chemical plants and nuclear power plants. In an interactively complex system, independent failures occur and interact in unexpected, non-linear, incomprehensible ways so that they defeat safety defenses that are in place. If the system is also tightly coupled, the initial failures propagate quickly and uncontrollably, resulting in cascades of failures that lead to a major breakdown. It is this combination of interactive complexity and tight coupling in some systems that make accidents inevitable or "normal". Some organizations are interactively complex but not tightly coupled: in a large university, for example, complex and unexpected interactions abound in the activities of students and staff. Yet initial failures (e.g. a boycott or strike) rarely lead to a major breakdown because of the slack and flexibility in the system (e.g. classes can be rescheduled) – the

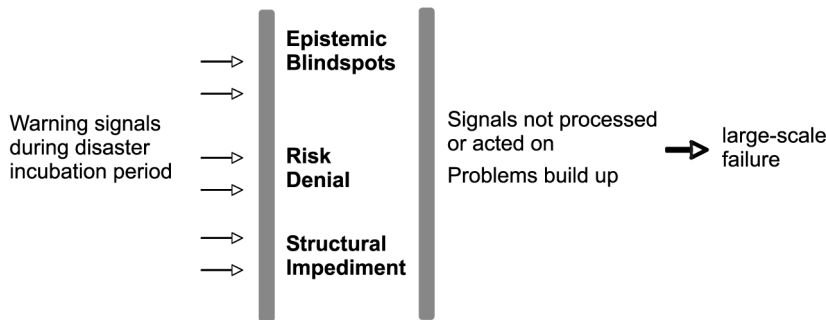


Figure 1.
Information impairments
and organizational failures

organization is loosely coupled. Only when systems are complex and tightly coupled are accidents unavoidable, although rare.

Accidents also occur in non-complex, low technology work settings. Rasmussen (1997) describes how accidents can happen when work practices migrate beyond the boundary of safe and acceptable performance. In any work system, groups and individuals search for work practices within boundaries formed by criteria such as cost effectiveness, work load, joy of exploration, risk of failure, and so on. Over time, work practices drift or migrate under the influence of two sets of forces. The first moves work practices towards least effort, so that the work can be completed with a minimum of mental and physical effort. The second is management pressure that moves work practices towards cost efficiency. The combined effect is that work practices drift towards and perhaps beyond the boundary of safety.

Can organizational disasters be foreseen? The surprising answer is yes. According to Turner and Pidgeon (1997), organizational disasters are “man-made”: they are neither chance events nor “acts of God” but “failures of foresight”. Turner analyzed 84 accident inquiry reports published by the British Government over an eleven-year period. He found that disasters develop over long incubation periods during which warning signals fail to be noticed. Four scenarios are common during the incubation period:

- (1) events are unnoticed or misunderstood because of erroneous assumptions;
- (2) events are unnoticed or misunderstood because of difficulties of handling information in complex situations;
- (3) effective violation of precautions are unnoticed because of ambiguous regulations or uncertainty about how to deal with violations; and
- (4) events are unnoticed or misunderstood because of a reluctance to fear the worst outcome (Turner and Pidgeon, 1997).

Information is often available but not attended to because the relevant information was buried in a mass of irrelevant information; the information was only presented at the moment of crisis; the recipient adopted a “passive” mode of administrative response to the issue; or the recipient could not put the information together creatively (Turner and Pidgeon, 1997, pp. 53-4).

Based on our review of the structure and dynamic of organizational disasters we identify three major types of information impairments. We describe each of them with the help of recent examples in section 3. Section 4 then offers some explanations of why they occur and how they can be managed.

3. Information impairments

3.1 Epistemic blind spots

A stream of warning signals is not heeded because the information does not fit existing beliefs, or because there is no frame of reference for the warnings to be recognized.

In the months preceding the September 11 attacks, US intelligence organizations have been receiving a succession of reports on the possibility of terrorist attacks within the USA that could involve the use of aircraft as weapons (US Senate, 2002a). On July 10, 2001, an FBI agent in Phoenix sent a memo to several colleagues expressing concern

that there was a coordinated effort by Bin Laden to send students to the USA for civil aviation training. In August 2001, the FBI's Minneapolis field office detained Zacarias Moussaoui, a French national who had enrolled in flight training in Minnesota, and who was suspected of being involved in a hijacking plot. Prior to September 11, intelligence organizations had information linking Khalid Shaykh Mohammed (KSM), now identified as the mastermind of the attacks, to Bin Laden, and to terrorist plans to use aircraft as weapons. However, the monitoring of KSM was limited to his location, rather than his activities. An August 6, 2001 Presidential Daily Brief titled "Bin Laden Determined to Strike in US" reported that since 1997 Bin Laden had wanted to conduct terrorist attacks in the USA, following the example of the World Trade Center bomber to "bring the fighting to America". The 9/11 Commission Report noted that "the system was blinking red" in the summer of 2001, but these warnings did not lead to action that could have averted the attacks (The 9/11 Commission, 2004). The general belief of US intelligence in 2001 was that an attack was more likely to occur overseas, possibly in Saudi Arabia and Israel. Intelligence information and related events shaped the thinking about where an attack was likely to occur. In fact, FBI agents in Yemen investigating the bombing of *USS Cole* in 2000 were told to leave the country because of concern about a possible attack. The belief that an attack would happen overseas was also expressed in numerous statements made by senior officials, including the National Security Advisor, the Deputy National Security Advisor, the Deputy Secretary of State, the Deputy Secretary of Defense, and FBI's Assistant Director for Counterterrorism (US Senate, 2002a, pp. 208-209).

The US Congressional Subcommittee investigating the fall of Enron concluded that:

[...] there were more than a dozen red flags that should have caused the Enron Board to ask hard questions, examine Enron policies, and consider changing course. Those red flags were not heeded (US Senate, 2002b, p. 59).

The investigation found that the Board received substantial information about Enron's activities and explicitly authorized many of the improper transactions. During the 1990s, Enron had created an online trading business that bought and sold contracts for energy products. Enron believed that to succeed it would need to access significant lines of credit to settle its contracts daily, and to reduce the large quarterly earnings fluctuations, which affected its credit ratings. To address these financial needs, Enron developed a number of practices, including "prepays", an "asset light" strategy, and the "monetizing" of its assets. Because it was hard to find parties willing to invest in Enron assets and bear the significant risks involved, Enron began to sell or syndicate its assets, not to independent third parties, but to "unconsolidated affiliates". These were entities that were not on Enron's financial statements but were so closely associated that their assets were considered part of Enron's own holdings. When warning signals appeared about these methods, Board members did not see them as such: they had developed the shared belief that these practices were a necessary part of doing business at Enron. In the end, the Board knowingly allowed Enron to move at least \$27 billion or almost half of its assets off balance sheet.

Epistemic blind spots arise because humans attend to and process information selectively. People tend to favor information that confirms their beliefs. When information contradicts their beliefs, rather than consider how their beliefs may need to change, people often choose to ignore the information, question its reliability, or

re-interpret its significance (Choo, 2006). Moreover, many organizations tacitly follow a justificationist approach in their decision-making processes. A “justificationist” organization holds its beliefs as being incontestable and during decision making looks for evidence that supports its beliefs and decision premises (Moldoveanu, 2002). It might ignore information that contradicts its premises, or it might strengthen its theories in order to account for the contrary evidence. A justificationist organization will rarely abandon its beliefs or mental model in favor of another.

3.2 Risk denial

Warning signals and events are discounted because of values, norms, and priorities that influence the evaluation and interpretation of information, so that no corrective action is taken.

In September 2004, Merck initiated the largest prescription-drug withdrawal in history. After more than 80 million patients had taken Vioxx for arthritis pain since 1999, the company withdrew the drug because of an excessive risk of heart attack and stroke. As early as 2000, the *New England Journal of Medicine* had published the results of a Merck trial, which showed that patients taking Vioxx were four times as likely to have a heart attack or stroke as patients taking naproxen, a competing drug (Bombardier *et al.*, 2000). Dr Edward Scolnick (then Merck’s chief scientist) had e-mailed to colleagues lamenting that the cardiovascular risks with Vioxx “are clearly there”. Merck argued that the difference was due to the protective effects of naproxen and not danger from its drug. In 2001, the *Journal of the American Medical Association* published a study by Cleveland Clinic researchers which found that the “available data raise a cautionary flag about the risk of cardiovascular events” with Vioxx and other COX-2 inhibitors (Mukherjee *et al.*, 2001). Merck did not answer the call for more studies to be done. In 2002, *The Lancet* published a study that found a significantly increased risk of cardiovascular death among new users of Vioxx compared with patients not using COX-2 inhibitors (Ray *et al.*, 2002). Karha and Topol (2004) described Merck’s reaction thus:

Each time that these data were presented, Merck claimed that the epidemiologic studies were flawed ... Merck opted to ignore the warning signs and [continued to] market Vioxx to consumers (Karha and Topol, 2004, p. 934).

In 2004, Merck was testing whether Vioxx could also prevent a recurrence of polyps in the colon. An external panel overseeing the clinical trial recommended stopping the trial because patients on the drug were twice as likely to have a heart attack or stroke as those on a placebo (Bresalier *et al.*, 2005). Merck decided to withdraw Vioxx, four years after the introduction of the blockbuster drug.

In February 1995, one of England’s oldest merchant banks was bankrupted by \$1 billion of unauthorized trading losses. The Bank of England report on the collapse of Barings Bank concluded that “a number of warning signs were present” but that “individuals in a number of different departments failed to face up to, or follow up on, identified problems” (GBBBS, 1995, sec. 13.12). In mid-1994, an internal audit of BFS (Baring Futures Singapore) reported as unsatisfactory that Nick Leeson was in charge of both front office and back office at BFS, and recommended a separation of the two roles. This report was regarded as important and was seen by the CEO of Baring Investment Bank Group, Group Finance Director, Director of Group Treasury and

Risk, and the Chief Operating Officer. Yet by February 1995 nothing was done to segregate duties at BFS. In January 1995, SIMEX (Singapore International Monetary Exchange) sent two formal letters to BFS about a possible violation of SIMEX rules and the ability of BFS to fund its margin calls. There was no investigation into these concerns. During all this time, Barings in London continued to fund the trading of BFS: significant funds were remitted regularly to BFS without knowing how they were being applied. Senior management continued to act on these requests without question, even as the level of funding increased and the lack of information persisted. The trading losses deepened rapidly and Barings Bank was sold for a pound sterling in March 1995. That Nick Leeson was able to hide his trading mistakes for so long was due to Barings' perception that the futures business, originally a one-person operation, needed to rely on an instinctive style of management. The bank failed to recognize that the norm of intuitive management was no longer appropriate when the operation expanded. Instead, Barings saw Leeson as the golden boy who would help the firm gain profits in the emerging Southeast Asian markets. Partly because of their regard for him, Leeson's managers discounted early warning signs. Moreover, Barings executives valued speed in decision making, and were willing to move quickly to take advantage of market opportunities without establishing a sufficiently rigorous system of controls.

Unlike epistemic blind spots, in situations of risk denial, warning signals and precursor incidents are registered – often formally as reports or letters – but their significance as warnings is denied or discounted so that no corrective action is taken. We may postulate reasons why managers decide not to heed early warnings: they think the risk is small or acceptable; they feel they can control or ride out the situation; they do not want to admit or expose their mistakes; and so on. Taking action to correct or prevent mistakes requires courage and resolve, and it is often easier not to acknowledge that there is a problem.

3.3 Structural impediment

Warning signals are recognized as such but organizational response is hobbled by structural rules, roles, and differentiation, so that information is incomplete and the response is ineffective.

On February 1, 2003, the space shuttle *Columbia* broke up while re-entering the earth's atmosphere. The physical cause of the accident was a breach in the left wing caused by insulation foam that had shed from the external fuel tank and struck the wing. The breach allowed superheated air to penetrate the wing during re-entry and destroy the internal aluminum structure. During *Columbia's* launch, the foam strike was caught on film but without a clear view of the damaged area. Three requests for imagery were made to obtain additional information about the extent of damage caused by the sizable debris – all three requests were turned down (CAIB, 2003). The first request was from the Intercenter Photo Working Group on the day after the launch. It was made in person by the chair of the Group to the Shuttle Program Manager for Launch Integration at Kennedy Space Center. The second request happened three days later by a manager of United Space Alliance (the shuttle's sub-contractor), as a result of concerns conveyed by his employees in the Debris Assessment Team. The manager telephoned Head, Space Shuttle Systems Integration at Johnson Space Center to ask

what it would take to get imagery of *Columbia* on orbit. The third request was also made the same day by the chair of the Debris Assessment Team who e-mailed the Manager, Shuttle Engineering Office, Johnson Engineering Directorate asking for outside assistance to get imagery that would help analysis. All three requests were cancelled by the Mission Management Team (MMT) for the following reasons. First, the calls were made without authorization from the MMT chair or they were not made to the designated liaisons for such requests – in other words, the requests did not follow “proper channels.” Second, MMT members did not see a requirement for such a request because they did not think that foam striking the shuttle would pose a critical threat. Third, MMT was concerned that obtaining imagery would delay mission schedule.

In May 2003, a five-year-old boy was admitted to the Children’s Hospital, Boston for elective neurosurgery to treat epilepsy. The surgery went well and the patient was transferred to the medical intensive care unit (MICU). In the evening the boy developed a seizure while still under anesthesia. The nurse called the Epilepsy Fellow listed as the patient’s physician. By phone, the Epilepsy Fellow ordered a number of doses of medication lower than what was called for by standard protocol, hoping that a small dose would be sufficient without interfering with the data they needed to gather for the next phase. When the Neurological Resident arrived he was alarmed at the low doses of medication but did not intervene. Later, the MICU Fellow was also surprised at the low dosage but was told by the nurse that the seizure was being managed by the Epilepsy Fellow and the Neurological Resident. The MICU Fellow then spoke on the phone with the Epilepsy Fellow who expressed concern that higher doses would adversely affect the subsequent investigation. The MICU Fellow felt that it was the Epilepsy Fellow’s call to make. The boy’s seizure continued and the MICU Fellow called for the MICU Attending Physician. When she arrived, she noticed that the patient had already stopped breathing. In their analysis of what went wrong, Snook and Connor (2005) wrote:

Picture five doctors and several nurses all standing around the hospital bed of a five-year-old little boy suffering from full body seizure. The protocol was clear and yet not followed. In this hyper-complex, best-in-practice organization, extreme levels of both vertical and horizontal differentiation had created . . . conditions for structurally induced inaction, with tragic results (Snook and Connor, 2005, p. 187).

Vertical differentiation was inherent in the strong hierarchical differences in the medical profession:

[...] nurses defer to interns, who defer to residents, who defer to fellows and attending physicians. For example, even though the Neurological Resident was alarmed at the low doses of medication, he did not intervene (Snook and Connor, 2005, p. 187).

Horizontal differentiation existed across functions:

[...] surgeons owned the surgical piece, epilepsy specialists concentrated on the impact medication might have on the phase 2 of their treatment plan, and intensive care staff deferred to the large team of outside specialists . . . The responsibility had become so diffuse that no one felt personally in charge of the boy’s care (Snook and Connor, 2005, p. 187).

The two accidents discussed above show how the structure of an organization could impede the perception and flow of warning signals and responses. Many organizations

point to the difficulty of recognizing weak signals of impending trouble. But what makes these signals weak? Snook and Connor (2005) assert that:

[...] ultimately, what makes a signal weak is that organizational actors perceive them to be that way. When faced with particularly ambiguous or unusual events, ones that don't necessarily fit the original design or current method for organizing work, the very same structural mechanisms required to accomplish well-understood, cutting-edge core tasks can actually work to defeat appropriate responses ... As organizations become increasingly differentiated, as roles become increasingly specialized, the effective likelihood that an unforeseen, potentially troublesome event will fit neatly into an existing organizational silo or an individual specialist's role descriptive or cognitive frame is decreased (Snook and Connor, 2005, pp. 183-4).

4. Preventing organizational disasters

Reason (1997) presents an accident causation model in which accidents develop through three levels of the organization, the workplace, and the individual. The causal chain starts with organizational factors that are related to the culture and decision processes of the organization. At the workplace level, the effects of organizational factors are seen in conditions such as time pressure, insufficient resources, inadequate training, fatigue, and information overload. Finally, at the individual level, organizational and workplace factors combine with natural limitations of the human mind and body to result in errors that are at the sharp end of the accident. We described three kinds of information impairments in the last section. In this section, we identify some of the factors that can explain why these impairments are common and suggest remedial strategies to improve vigilance and resilience against accidents. We structure our discussion by looking at the individual, the work group, and the organization respectively.

4.1 *Individual factors: cognitive heuristics and biases*

When individuals process information to make judgments under conditions of uncertainty, they rely on mental shortcuts or heuristics that economize on cognitive effort but that can result in systematic biases (Tversky and Kahneman, 1974). Research has identified many such information biases. For example, we prefer information that confirms our beliefs, process information selectively so as to justify desired conclusions, and over-rely on stereotypes or easily retrievable information (Gilovich *et al.*, 2002). The unconscious reliance on habitual heuristics can help explain the existence of epistemic blind spots that make us overlook or fail to process crucial information. Individuals in organizations can increase their cognitive alertness by first being aware of the kinds of biases that distort our judgments and decision making. Some methods to offset these tendencies and reduce epistemic blind-spots include: applying different frames of reference to look at a problem; using counterfactual reasoning to imagine improbable or unpopular outcomes; listening carefully to stakeholders and experts who have different points of view; and using theories and models to guide analysis. Underlying these methods, is a general commitment to ensure that information has been canvassed from a wide range of sources to represent a broad range of perspectives, and that this information has been evaluated and considered objectively.

When a course of action has gone very wrong, and objective information indicates that withdrawal is necessary to avoid further losses, many managers decide to persist, often pouring in more resources in an attempt to justify and protect their past decisions (Ross and Staw, 1993). Although past decisions are sunk costs that are irrecoverable (Arkes and Blumer, 1985), they still weigh heavily in our minds, mainly because we do not want to admit error to ourselves, much less expose our mistakes to others. If facts challenge a project's viability, we find reasons to discredit the information. If the information is ambiguous, we select favorable facts that support the project. Culturally, we associate persistence with strong leaders who stay the course and view withdrawal as a sign of weakness. The sunk costs effect and the tendency to escalate commitments can explain why managers persist in a risky course of action that is going badly, despite having information that indicates that radical measures are required. How can managers know if they have crossed the line between determination and over-commitment? Staw and Ross (1987) suggest asking a few pointed questions:

- Do I have trouble defining what would constitute as failure for this decision?
- Would failure in this project radically change the way I think of myself as a manager?
- If I took over this job for the first time today and found this project going on, would I want to get rid of it?

4.2 Work group factors: groupthink and group polarization

For the work group, we are concerned with how a group's ability to seek and use information may be compromised by groupthink and group polarization. Groupthink occurs when people working in highly cohesive groups strive for concurrence to such an extent that it undermines their ability to seek and use information, and to consider alternative explanations (Janis, 1982). There are three symptoms of groupthink. First, group members share a feeling of invulnerability, which leads to optimism and a willingness to take risks. Second, group members are close-minded, collectively rationalizing or discounting aberrant information and maintaining stereotyped views of threats or rivals. Third, group members press toward uniformity, sustaining a shared impression of unanimity through self-censorship as well as direct pressure against dissenting views. We note that the symptoms of undue optimism, willingness to take risks, and discounting of discrepant information can all contribute to the condition of risk denial that we discussed earlier. Groupthink was identified recently as a cause of the faulty intelligence assessment on "weapons of mass destruction" in Iraq. The US Senate Select Committee on Intelligence Report found that intelligence community personnel "demonstrated several aspects of groupthink: examining few alternatives, selective gathering of information, pressure to conform with the group or withhold criticism, and collective rationalization" (US Senate, 2004, p. 18). Groupthink can be prevented. The same team of President Kennedy and his advisors that launched the disastrous Bay of Pigs invasion (a textbook example of groupthink) subsequently handled the 1962 Cuban Missile Crisis effectively, creating a model of crisis management.

Group polarization (Stoner, 1968) happens when a group collectively makes a decision that is more risky than what each member would have done on their own. The result of group polarization is a failure to take into account the true risk of a course of

action followed by a shift towards riskier decision making. An explanation of group polarization is the process of social comparison: we compare our decision with the decision of others. Initially we may think of ourselves as risk-taking, especially when this is considered a valued trait in the organization or society. When, during subsequent group discussion, we discover that we are not particularly risky compared to others, we then increase the level of risk of our decision when asked to remake the decision.

Groupthink and group polarization can be controlled. The basic strategies here would be to encourage openness among group members, and to reduce social pressures to conform to the majority view or the leader's preferences. To overcome conformity tendencies, the leader should create a group environment that encourages the frank exchange of dissimilar views. The leader should be impartial and avoid stating preferences at the outset. To counter close-mindedness, the group should actively seek information from outside experts, including those who can challenge the group's core views. The group could divide into multiple subgroups that work on the same problem with different assumptions. A member could play the role of a devil's advocate who looks out for missing information, doubtful assumptions, and flawed reasoning.

4.3 Organizational factors: bureaucratic culture and information dispersion

The set of values and priorities in an organization's culture can determine how warning information is evaluated, how responsibility is defined, and whether action is taken. Westrum (1992) contrasts different types of information cultures in organizations according to how well they notice information and address failure and responsibility. In an organization with a bureaucratic information culture, responsibility is compartmentalized; information sharing is permitted but not facilitated or encouraged; new information including warning signals tend to get lost or be submerged in other information so that they are not noticed. In contrast, an organization with a generative information culture would actively seek out new or discrepant information, share responsibility between organizational units, reward information sharing, and welcome new ideas or alternative interpretations (Westrum, 1992, p. 402).

Turner and Pidgeon (1997) found that it was common for disasters to happen:

[...] when a large complex problem, the limits of which were difficult to specify, was being dealt with by a number of groups and individuals usually operating in separate organizations (Turner, 1976, p. 384).

Situations of this kind are said to have information that is "variably disjunctive", where:

[...] a number of parties handling a problem are unable to obtain precisely the same information about the problem so that many differing interpretations of the problem exist (Turner, 1978, p. 50).

This information dispersion is a consequence of organizational structure. Thus, problems that produce disasters can ramify in unexpected ways because dispersed groups have diverse, non-overlapping pieces of information: each group has partial information that is incomprehensible because crucial pieces are missing. It is the distribution and flow of information that affects an organization's ability to detect, mitigate, and recover from failures:

[...] it is important to pay attention, not just to the aggregate amount of information which is available before a disaster, but also to the distribution of this information, to the structures and communication networks within which it is located, and to the nature and extent of the boundaries which impede the flow of this information (Turner and Pidgeon, 1997, p. 91).

One countermeasure is to increase information redundancy between organizational units so that they have access to common information that goes beyond their immediate operational needs or functional specializations. This can expand the organization's peripheral vision and its ability to discern and react to danger signals.

As a general strategy, organizations need to cultivate a safety-oriented information culture. Safety culture is the set of beliefs, norms and practices through which people perceive and work with risk and safety (Pidgeon and O'Leary, 2000). Research on "high reliability organizations" (such as nuclear aircraft carriers and hospital emergency departments that do risky work but remain relatively accident-free) reveal that these organizations manage the unexpected by acting mindfully:

[...] they organize themselves in such a way that they are better able to notice the unexpected in the making and halt its development. If they have difficulty in halting the development, they focus on containing it. And if some of the unexpected breaks through the containment, they focus on resilience and swift restoration of system functioning (Weick and Sutcliffe, 2001, p. 3).

The key difference between the way that high reliability organizations and other organizations manage the unexpected occurs in the earliest stages, when warning signals are still weak and ambiguous. While the general tendency is to react to weak signals with a weak response, high reliability organizations act counter-intuitively by developing the capability to see the significance of weak signals and to respond strongly to weak signals.

High reliability organizations observe five information priorities. They are preoccupied with the possibility of failure, and they do what they can to avoid it – they encourage error reporting, analyze experiences of near misses, and resist complacency. They recognize that the world is complex and rather than accepting simplified interpretations, they seek a more complete and nuanced picture of what is happening. They are attentive to operations at the front line, so that they can notice anomalies early while they are still tractable and can be isolated. They develop capabilities to detect, contain, and bounce back from errors; and so create a commitment to resilience. They push decision-making authority to the people with the most expertise, regardless of their rank.

5. Summary

We summarize our discussion of information impairments, their causes and possible remedial strategies in Table I.

While we have discussed blind spots, risk denials, and structural impediments as information impairments, we recognize that they are outgrowths of the mechanisms we have developed to cope with risk and uncertainty. Thus, cognitive heuristics economize on mental effort, enabling us to make judgments quickly and correctly enough. Risk assessments allow us to work through hazardous situations where information is incomplete and ambiguous. Divisional structures and functional differentiation permit organizations to grow and specialize in increasingly complex environments. On the one

Information impairments	Causes	Remedial strategies
Epistemic blind spots	Heuristics and biases	Gather information broadly and evaluate information objectively
	Escalation of commitment	Use alternative frames and counterfactual reasoning
Risk denial	Groupthink	Create an open climate for discussion and reduce pressures to conform
	Group polarization	Avoid insulating the group from outside criticism
Structural impediment	Bureaucratic culture	Develop a “high reliability” culture that can sense and respond early to warning anomalies
	Information dispersion	Actively encourage information sharing and managed information redundancy

Table I.
Summary of information
impairments and
remedial strategies

hand, these mechanisms constitute a way of seeing and acting in the world according to current beliefs and expectations. On the other hand, they can diminish the organization's ability to recognize and respond to signals and events that presage failure. Ultimately, preventing organizational disasters requires a vigilant information culture that balances the need for efficient operations with the alertness to attend to the surprising and the abnormal (Choo, 2005). Where there is a fundamental understanding that failures are a realistic and manageable threat, then, there is the collective resolve to search for, and then deal with, the precursor conditions.

References

- Arkes, H.R. and Blumer, C. (1985), “The psychology of sunk cost”, *Organizational Behavior and Human Decision Processes*, Vol. 35 No. 1, pp. 124-40.
- Bombardier, C., Laine, L., Reicin, A. and Shapiro, D. (2000), “Comparison of upper gastrointestinal toxicity of Rofecoxib and Naproxen in patients with rheumatoid arthritis”, *New England Journal of Medicine*, Vol. 343 No. 21, pp. 1520-8.
- Bresalier, R.S., Sandler, R.S., Hui, Q., Bolognese, J.A. and Oxenius, B. (2005), “Cardiovascular events associated with Rofecoxib in a colorectal adenoma chemoprevention trial”, *New England Journal of Medicine*, Vol. 352 No. 11, pp. 1092-102.
- CAIB (Columbia Accident Investigation Board) (2003), *Columbia Accident Investigation Board Report*, Vol. 1, Government Printing Office, Washington, DC.
- Choo, C.W. (2005), “Information failures and organizational disasters”, *Sloan Management Review*, Vol. 46 No. 3, pp. 8-10.
- Choo, C.W. (2006), *The Knowing Organization: How Organizations Use Information to Construct Meaning, Create Knowledge, and Make Decisions*, 2nd ed., Oxford University Press, New York, NY.
- Gilovich, T., Griffin, D. and Kahneman, D. (Eds) (2002), *Heuristics and Biases: The Psychology of Intuitive Judgment*, Cambridge University Press, Cambridge.
- GBBBS (Great Britain Board of Banking Supervision) (1995), *Report of the Board of Banking Supervision Inquiry into the Circumstances of the Collapse of Barings. House of Common Papers 1994-95*, The Stationery Office Books, London.

-
- Janis, I. (1982), *Groupthink: Psychological Studies of Policy Decision*, Houghton Mifflin, Boston, MA.
- Karha, J. and Topol, E.J. (2004), "The sad story of Vioxx, and what we should learn from it", *Cleveland Clinic Journal of Medicine*, Vol. 71 No. 12, pp. 934-9.
- Moldoveanu, M. (2002), "Epistemology in action", in Choo, C.W. and Bontis, N. (Eds), *The Strategic Management of Intellectual Capital and Organizational Knowledge*, Oxford University Press, New York, NY, pp. 403-20.
- Mukherjee, D.M., Nissen, S.E. and Topol, E.J. (2001), "Risk of cardiovascular events associated with selective COX-2 inhibitors", *Journal of the American Medical Association*, Vol. 286, pp. 954-9.
- Perrow, C. (1999), *Normal Accidents: Living With High Risk Technologies*, Princeton University Press, Princeton, NJ.
- Pidgeon, N. and O'Leary, M. (2000), "Man-made disasters: why technology and organizations (sometimes) fail", *Safety Science*, Vol. 34 Nos 1-3, pp. 15-30.
- Rasmussen, J. (1997), "Risk management in a dynamic society: a modeling problem", *Safety Science*, Vol. 27 Nos 2/3, pp. 183-213.
- Ray, W.A., Stein, C.M., Hall, K., Daugherty, J.R. and Griffin, M.R. (2002), "Non-steroidal anti-inflammatory drugs and risk of serious coronary heart disease: an observational cohort study", *The Lancet*, Vol. 359, pp. 118-23.
- Reason, J.T. (1997), *Managing Risks of Organizational Accidents*, Ashgate Publishing, London.
- Ross, J. and Staw, B.M. (1993), "Organizational escalation and exit: lessons from the Shoreham Nuclear Power Plant", *Academy of Management Journal*, Vol. 36 No. 4, pp. 701-32.
- Snook, S.A. and Connor, J.C. (2005), "The price of progress: structurally induced inaction", in Starbuck, W.H. and Farjoun, M. (Eds), *Organization at the Limit*, Blackwell Publishing, Oxford, pp. 178-201.
- Staw, B.M. and Ross, J. (1987), "Knowing when to pull the plug", *Harvard Business Review*, Vol. 65 No. 2, pp. 68-74.
- Stoner, J. (1968), "Risky and cautious shifts in group decisions: the influence of widely held values", *Journal of Experimental Social Psychology*, Vol. 4, pp. 442-59.
- The 9/11 Commission (2004), *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, US Government Printing Office, Washington, DC.
- Turner, B.A. (1976), "The organizational and interorganizational development of disasters", *Administrative Science Quarterly*, Vol. 21 No. 3, pp. 378-97.
- Turner, B.A. (1978), *Man-Made Disasters*, Wykeham, London.
- Turner, B.A. and Pidgeon, N.F. (1997), *Man-Made Disasters*, 2nd ed., Butterworth-Heinemann, Oxford.
- Tversky, A. and Kahneman, D. (1974), "Judgment under uncertainty: heuristics and biases", *Science*, Vol. 185 No. 4157, pp. 1124-31.
- US Senate (2002a), *Select Committee on Intelligence and US House Permanent Select Committee on Intelligence. Joint Inquiry into Intelligence Community's Activities Before and After the Terrorist Attacks of September 11, 2001*, US Government Printing Office, Washington, DC.
- US Senate (2002b), *Committee on Government Affairs – Permanent Subcommittee on Investigations. Role of The Board of Directors in Enron's Collapse*, US Government Printing Office, Washington, DC.

-
- US Senate (2004), *Select Committee on Intelligence. Report on the US Intelligence Community's Prewar Intelligence Assessments on Iraq*, Government Printing Office, Washington, DC.
- Weick, K.E. and Sutcliffe, K.M. (2001), *Managing the Unexpected: Assuring High Performance in an Age of Complexity*, Jossey-Bass, San Francisco, CA.
- Westrum, R. (1992), "Cultures with requisite imagination", in Wise, J.A., Hopkin, V.D. and Stager, P. (Eds), *Verification and Validation of Complex Systems: Human Factors Issues*, Springer-Verlag, Berlin, pp. 401-16.

Further reading

- Kahneman, D. and Tversky, A. (Eds.) (2000), *Choices, Values and Frames*, Cambridge University Press, Cambridge.
- La Porte, T.R. (1996), "High reliability organizations: unlikely, demanding and at risk", *Journal of Contingencies and Crisis Management*, Vol. 4 No. 2, pp. 60-71.
- Roberts, K.H. and Bea, R. (2001), "Must accidents happen? Lessons from high-reliability organizations", *Academy of Management Executive*, Vol. 15 No. 3, pp. 70-9.
- Sunstein, C.R. (2003), *Why Societies Need Dissent*, Harvard University Press, Cambridge, MA.

Corresponding author

Chun Wei Choo can be contacted at: cw.choo@utoronto.ca