Tommaso Palermo

Technoculture: risk reporting and analysis at a large airline

Book section

Tommaso Palermo
Department of Accounting
London School of Economics and Political Science
Tel: +44 (0)20 7849 4630
Email: t.palermo@lse.ac.uk

Book chapter, forthcoming, in Michael Power (Ed.), Riskwork - The everyday life of risk management, Oxford University Press

Technoculture: Risk reporting and analysis at a large airline

> "If they get into the whistle-blower line then they've gone too far; you don't need a whistle, we give them a whole orchestra to play with, the whistle's the last thing on our list." (Senior manager, Safety Department at *Airline*)

Enterprise risk management frameworks portray risk management as a standardised process of risk identification, reporting and control (see IRM/AIRMIC/ALARM, 2002; COSO, 2004; ISO, 2009). However, risk identification, reporting and control are multi-faceted practices: How can individuals understand what qualifies as a risk to be reported (Weick & Sutcliffe, 2007; Macrae, 2007a, 2007b)? How can organisations address the numerous biases that inhibit the ability to discuss risks and failures (Kaplan & Mikes, 2012)? What is the right balance between the use of incentive structures that recognize financial and legal liability for risk and adoption of 'no-blame' cultures (Hood & Jones, 1996)? What are the consequences of 'speaking up' in contexts that are subject to

increased demands for public scrutiny (Power, 2007)? And how do executives react to 'bad news' (Simons, 1999)?

Organisations often address these issues of risk identification and escalation by prescribing structural changes and by adopting new control technologies such as whistleblowing, oversight functions, formal values-based controls, reporting and monitoring systems. Demands for improvement are also made in terms of 'softer' elements such as corporate (risk) cultures and ethics (e.g., Weick & Sutcliffe, 2007; Mikes & Kaplan, 2012; Power et al., 2013). This chapter explores the relations between control technologies and organisational culture and how their mutual interdependence influences the flow of information between front-line, staff functions (e.g., risk, compliance, internal audit) and top managers. The focus of this chapter can be characterized in terms of the following questions: When and how do (and can) people feel free to 'speak up' and report risks? What kinds of technologies and cultures enable risk reporting and analysis? How does their operation define specific ways of working with risk?

In the spirit of this volume, the chapter does not draw on a specific theoretical lens or body of the literature. The chapter rather provides an empirical account of riskwork within the Safety Department of a large airline company (hereafter anonymised as *Airline*). As suggested in the initial quote, the Safety Department provides to members of staff 'a whole orchestra' to play with. Following a brief account of the data collection and research methods, the chapter begins by illustrating the practices that constitute such an 'orchestra'. Secondly, it develops the notion of *technoculture*, which aims to capture the way in which a specific notion of corporate culture becomes hard-wired, materialized and operationally

expressed by reporting and other managerial systems. Thirdly, the chapter shows how this notion of *technoculture* helps us to understand riskwork by drawing on two vignettes, which illustrate how safety data are captured, used and acted upon.

Methods

The author collected qualitative data from the Safety Department of a major airline company, headquartered in the UK and operating a wide range of national and international flights[1]. Data was gathered from face-to-face meetings with six members of the Safety Department (including the Director, her deputy and four members of staff from three distinct teams) and public documents such as corporate reports and media articles. Formal interviews were complemented by informal conversations with the Director and other members of staff. Interviews with the Director and her deputy were recorded and then transcribed, while detailed notes were taken during the other meetings (therefore, unless specified otherwise, all quotes in this chapter comes from the two senior managers).

The headquarters of *Airline* were visited on two distinct periods of time (May 2013 and May 2014), thus providing a tentative sense of the longitudinal development of safety risk workstreams. The company visits also included comprehensive exposure to different office spaces, including the working environment of senior managers, managers and members of staff from different functions (e.g., safety, commercial, engineers etc.), crew rooms and the

[1] Data collection was initially carried out in the context of a broader project on 'risk culture in financial organisations' (together with Mike Power (LSE) and Simon Ashby (Plymouth Business School)).

corporate canteen. Moreover, it was possible to observe the functioning of the safety reporting system (with simulated data), a demonstration of the use of smart phone apps to access the internal reporting system, as well as a video related to the induction programme for new hires. Observation of such elements complemented data collected from interviews and documents. As a research strategy, the approach adopted reflects the spirit of calls for closer attention to the field in research on '(risk) work' in organisation studies (Barley & Kunda, 2001).

Data collected from the company were also complemented by information obtained directly from senior representatives of the UK aviation regulatory agency. Two meetings took place in July and October 2014. The conversations focused on the regulation and oversight of safety risks within the airline sector. Finally, interview material was supplemented by an analysis of publicly available material such as policy documents and corporate presentations.

Practices

Just culture

The notion of just culture was reiterated several times in relation to the work done within the Safety Department. This notion has been articulated in prior work on safety and crisis management in relation to the way in which organisations handle blame and punishment, and how this can influence what gets reported (Reason, 1997; Weick & Sutcliffe, 2007).

Weick and Sutcliffe (2007: 131) describe just culture as "an atmosphere of trust in which people are encouraged, even rewarded, for providing essential safety – related information – but in which they are clear about where the line must be drawn between acceptable and unacceptable behavior." One interviewee defined just culture in her own way as follows:

> "Just culture is a culture whereby an individual can make an honest mistake or perhaps an omission but where wilful violations are not tolerated […] Because you can't have a no-blame culture whereby I want X to tell me if he's made a mistake and I promise you if you've made a mistake I won't do anything, okay […] That is not good in the interests of the individual, nor the individual's colleagues, nor the interests of the business; there has to be this *idea of justice*. And that means that we can have a *fair hearing*." (Emphasis added)

So the just culture concept recognizes that *Airline* has responsibility to identify the causal factors of a safety event to reduce the risk of recurrence, and also acknowledges that human failures can be the root cause of an event. But it also recognizes that if individuals operate in line with company's procedures, training and experience, then the failure will not necessarily result in disciplinary sanctions. Just culture is strongly intertwined with attitudes to internal reporting that reflect confidence in the possibility of having what interviewees called a "fair hearing." As put by a senior manager:

> "If it's been a genuine mistake, if it's been a genuine omission, okay and it's commensurate with your training and skill level, then we need to learn

> from it. We might retrain you, we might give you some additional support but you fear not."

Just culture, and its development, is related to organisational culture (interviewees mention the famous expression attributed to Edgar Schein: 'the way we do things around here'), and so-called 'soft' elements such as 'energy' and 'leadership', the quality and amount of 'dialogue' between employees and senior management as well as among employees themselves. One senior manager often made reference to the formation of a "contract of understanding" between the employee, the company and its senior management. Using her words, "we want you to report, we need that information to make your environment safer … But for you to report you need to understand how we're going to behave." The description of such a cultural contract echoes discussions of culture as ways of knowing and sensemaking. Paraphrasing Schein, the key question is not so much how "we do things around here", but "how we develop expectations around here" (Weick & Sutcliffe, 2007: 119).

But just culture is also based on physical processes and procedures that contribute to the identification of a risk, its reporting as well as understanding whether it's a "genuine mistake" or "a willful negligent act." In short, the systemic component of just culture consists of a number of reporting and monitoring technologies. The following sections focus on three such technologies that share a set of commonalities, namely a strong emphasis on encouraging internal reporting, the availability of large datasets, and the relevance of data analysis skills.

Safety Reporting

The Safety Reporting[2] (SR) system is a web application that is designed to engage all staff in safety management and incident reporting. It is a hub for reporting safety issues, which is capable of handling various processes such as event investigation, risk assessment and analysis, and peer reviews. SR has more than 10,000 users and almost 30,000 reports were recorded in the year preceding the research. The purpose of the system is to allow personnel to report any safety matters and it is adjusted to the different areas of the organizations (e.g., pilots, crew members and other personnel). The underlying philosophy is that any and all matters should be reported. As put by a senior manager:

> "So each area of the organisation has a dedicated report form on which they can report any safety matters, whether they're … you know, if I take the pilot example, the pilot will use it to report any incidents that occur or potential incidents that occur during their operation. He'll also report it for a trip hazard on the way into the office, he'll also use it if he was transferring from one airport to another in a taxi and the taxi driver was mad. So you know, they have these dedicated streams that are particular to each department."

[2] The name of the application has been modified to maintain anonymity.

Figure 7.1 provides an overview of the application functionalities and reporting process. All investigations start with an incident report filed by a member of staff (hereafter called the reporter). The system has pre-set event descriptors with over 2,000 combinations that can be chosen by the person reporting an event, while basic information is already automatically inserted (e.g., number of flight, crew members). The bottom half of the screen visualized by the reporter asks for details about the event type, which can be very granular. Let's suppose that a bird has hit the airplane. Crew members can access the reporting system remotely, where some details are already inserted (e.g., crew details). The reporter inserts information about the event type. Further questions will be selected by the system based on the input already given: for instance, the part of the plane that was struck, type of bird, estimated number of birds. The reporter can highlight if some information should be treated as confidential in case further investigation arises. The reporter can also use a red flag process to alert management to a potential safety risk that needs attention. The management then decides if the red flag warrants immediate attention.

Figure 7.1 here

The report can be closed immediately depending on the investigator's judgement about the relevance of the risk event. Alternatively the investigation can take more or less time depending on each case. In some cases explanatory reports can take several months as the investigators need to seek out help with operations, engineers and other functional experts. Indeed, requests for peer reviews are frequent. Information from experts is collected, stored and can be retrieved as needed in specific boxes within the system. The final report is sent out to various recipients who have been involved with the investigation. The

investigator can decide which parts of the report to disclose, who can receive the report, and which sections she would be able to see. If recommendations are raised by investigators, the reporter or other staff involved need to upload evidence that something has been done or the reasons why the recommendations were rejected.

Various reports can be flexibly created and published based on different parts of the investigation (e.g., descriptors, recommendations, actions, risk values etc.). The system also provides a platform to interact with regulators. Investigators can do a print screen of different parts of the investigation and hand this material to the regulators. As put by one investigator: "we just tell them, have a look yourself!". The reports can be used as factual evidence that something is a recurring problem in a specific context (e.g., a 'bad' airport), and may require regulatory attention.

Flight Data Monitoring

Pilots' performance is also monitored in real time through a Flight Data Monitoring (FDM) system. According to one member of the monitoring team, FM aims to provide a "non-punitive environment" to analyse data from black boxes. The investigations are carried out at central offices by a team of four people, all of whom had been flying pilots in the past, an element that helps to add "content and background" to the data analysis. As put by a member of the team, "otherwise we would not have credibility" in conversations with flying pilots.

The analysis can be triggered by a pilot asking for it, by a safety report being filed, or by the monitoring team directly. Even if a pilot is not asking for it, the flight management team should be able to start an investigation anyway. As put by one member of the team, "the pilot needs to file a report if there is a reportable event", but the team revising the data "would be able to pick up an anomaly anyway." FM is described as being not "malicious" in intent, but the data basically enables the reconstruction of all the actions that have been taken by a pilot. Using the words of a member of the monitoring team, the system allows them to "see if the pilot has done the right thing, for example in case of TCAS[3] if he was told to go down, did he actually go down?"

The key skill according to the monitoring team's members is related to data analysis. For example, an investigation can relate to turbulence that is considered excessive. The monitoring team examines the data, which can be presented in different forms such as a spreadsheet or 3D visualisations of the plane movement. If the problem cannot be figured out directly by the monitoring team, then the data is transferred to engineers. The opinion of engineers is normally sought anyway on the final document. The amount of information is significant, and a good investigator should be able to pick up the pieces of information that enable an explanation of the problem that has occurred, even if this information is not the most visible.

[3] Traffic Collision Avoidance System monitors the airspace around an aircraft for other aircraft equipped with a corresponding active transponder, and warns pilots of the presence of other aircraft which may present a threat of collision.

Fatigue Risk Management

The company has also developed a reporting process around fatigue issues, which since the early 2000s have been an increasingly prominent part of operational risk (e.g., including high risk events such as micro-sleep during critical phases of a flight). Fatigue Risk Management (FRM) is defined as a data-driven means of monitoring and managing fatigue-related safety risks to make sure that personnel are performing at an adequate level of alertness. Although there are regulations for fatigue risk management, an interviewee stated that "the boundaries are thin … there are a number of things that can be done within or outside the rules." For instance, a 12-hour break can be interpreted flexibly as it can be taken at any time: "but it is not the same 12 hours at night and 12 hours in the middle of the day." Therefore, as illustrated by one senior manager, "what [the airline] did then was to challenge the regulator on the basis of academically-accredited procedures and processes to say look, we think we can do this differently."

The fatigue risk management system consists of several different components: a fatigue risk management policy; a crew fatigue reporting mechanism with associated feedback; procedures and measures for assessing and monitoring fatigue levels; procedures for investigating, and recording incidents that are attributable wholly or in part to fatigue; processes for evaluating information on fatigue levels and fatigue-related incidents, undertaking interventions, and evaluating the effects of those interventions; awareness training programmes; and, finally, a performance audit plan. Once again, internal reporting is the key trigger for fatigue-related investigations. The data is based on detailed reports filed by pilots and crew members (around 6,000 reports in the year preceding my research)

which include elements such as details of current duty, previous duties, flying hours, night stops away from base, commute times, sickness records and other so-called 'hassle' factors.

FRM team members see themselves as internal consultants and produce "a huge amount of reporting every month" that aims to help decision-making, including commercially-sensitive issues such as flight scheduling. As in SR and FM described above, the team aimed to encourage a reporting culture around fatigue risks. The availability of large samples of data was seen as crucial to identify specific stress points, such as certain airports that are at the centre of many routes and therefore can cause more problems with assembling crews. The FRM team analyses the data and tries to find the root causes, often through predictive models with the help of SR information. In contrast to other safety teams, most of the FRM team members do not have a background as flying pilots; "being good with numbers" is instead the key skill required.

Technoculture

The four discrete but related safety practices of *Airline* suggest a specific view of the relation between culture and control technologies, summarised by the motif of *technoculture*. Far from being a fully developed concept, *technoculture* may be useful in moving forward the theoretical and empirical study of how, where and when risk management work takes place. Of course, 'technology' and 'culture' are topics that have been researched extensively in different ways and it would be over-ambitious to argue that

a new compound word is self-evidently descriptive. In fact, the analytical distinction between culture and technology can be challenged in the first place. On the one hand, an organisation can be seen as *being* a culture as opposed to *having* a culture (Alvesson, 2002: 24-29). According to this perspective, culture is not separable from other organisational properties, including technology. Rather, it permeates the entire organisation and is reproduced in formal structures, administrative processes, strategic plans and other, apparently technical, tasks and results-oriented activities. On the other hand, technology can be seen as a social product, rather than having a social impact once it is produced (Bijker et al., 1987). If one looks closely at those who work with technology (e.g., engineers), technical, economic, scientific, social and political considerations are intertwined right from the start of technology development (Callon, 1987). Apparently 'technical' phenomena are neither isolated nor static; they are characterised by dynamic socio-technical networks that can vary in terms of size and complexity, including multiple and various human and non-human components[4] (Hilgartner, 1992).

Empirical studies have also shown how culture and technology are entangled with one another. It is possible to provide three examples where, similar to *Airline*, technology refers not only to complex operations, but also to technologies of control such as rules that guide decisions about risks, work practices, procedural and hardware surveillance systems. The ethnographic study carried out by Kunda (1992) in a US high-tech corporation (called 'Tech') shows how corporate culture itself can be a technology of control. Multiple

[4] Hilgartner (1992) uses the example of auto-based transport, which includes entities that have physical existence such as tires and engines, human subjects such as drivers and regulators, and also less tangible elements such as traffic laws.

communication circuits constantly promoted Tech's 'way of doing things', defining not only required work behaviour but also rules for thoughts and feelings. The historical ethnographic analysis carried out by Vaughan (1996) on the Challenger disaster shows how the experimental character of the shuttle technology coupled with group-based risk assessment processes, ad-hoc hardware surveillance and measurement systems and standardised rules for decision-making across the organisation resulted in a cultural tendency to normalise technical anomalies (e.g., 'flying with flaws' at NASA). Finally, the study carried out by Macrae (2007a; 2007b) on the work of safety experts in the UK aviation sector suggests that the sheer complexity of airline operations together with an appreciation of the limits of incident reporting technologies contributed to the development of a distinct analytical culture characterised by scepticism, humility and caution. Safety people considered risk assessments to be the product of limited, and most likely flawed, knowledge and therefore continually open to change.

In line with studies such as these, the concept of *technoculture* demands that we avoid a dualism of technology and culture and that we explore the practices where they are entangled with one another. It suggests that neither culture nor technology are distinct features of the context in which safety experts work, but they are manifested and co-produced in specific places and times. Specifically, in this chapter, the expression *technoculture* is invoked to identify and explore three coterminous features that characterise the entanglement of technology and culture in *Airline*: 1) the hard-wiring of cultural values of safety into systems, processes and other visible artifacts; 2) the expansion of certain types of working interactions supported by reporting and monitoring

technologies; 3) the adoption of a business partnering approach by safety experts to build respect for safety values, people and technologies.

Hard-wiring culture

The just culture narrative is expressed in two mutually supportive pillars: on the one hand, a "cultural contract" between senior management and employees; on the other hand, processes and systems. The practical functioning of safety practices suggests that just culture does not float around in a set of principles or corporate values; it gets hard-wired into control technologies. Reporting and monitoring systems embody the ambivalence of just culture that promotes an atmosphere of trust, in which people are encouraged to provide essential risk information that is not blame-less. SR, for instance, is a highly forensic system that does "not allow any corners to hide." Staff members do not need to be 'good'; by and large, they are made 'good' by reporting and monitoring systems as the problems they report are likely to be picked up by the technology anyway. As put by one interviewee:

> "And the way we do that is through two things; positive encouragement and leverage. And the leverage comes from the system and the system is geared […] I liken it to a room with no corners … *you cannot hide anywhere* because there isn't a corner to hide in because the system drives that and it's auditable." (Emphasis added)

Technologies of control such as SR, FM and FRM are not intended to be "malicious" tools (a term used by a member of the flight data monitoring team) but rather should provide a non-punitive environment that encourages the reporting of any kind of issue. And yet, lurking in the background is the idea that issues will be picked up anyway through the system. As expressed by a senior manager in relation to the influence of technologies on just culture: "from the pilot's point of view, they know everything's being watched, so that also in a subtle way helps them be honest."

But senior managers stressed the difficulty to achieve control over individual actions through the use of monitoring technologies, incident reporting and investigation systems only. Just culture is also based on other 'soft' elements, including visible and sustained management attention to safety issues, which are the equivalent of the hard-wired flight data monitoring system put in place on the aircraft. These 'soft' elements can be materially traced in the organisation, similar to the symbols, rituals and other artefacts that are often associated to notions of corporate culture (Schein, 2004), and belief control systems (Simons, 1995). Interviewees continuously expressed the need for 'energy' and 'alchemy' on top of 'systems' by using metaphors and symbols that were cascaded down throughout the organisation. For instance, the need for a full understanding of just culture from employees and regulators was explained through the use of examples that referred to academic research in anthropology[5]. Corporate presentations (both public and internal)

[5] An example is related to the experience of indigenous people in Oceania, who witnessed the landing of planes and subsequently reproduced a rudimental airport waiting for airplanes to come and land. These people did not have a full understanding of how the airport/airplane system worked, although their attempt to reproduce the various components of an airport (e.g., runway, landing lights, control tower) was remarkable. In a similar way, a company would fail in safety management if people simply comply with the components

referred to symbols, graphs and diagrams elaborated in academic research (in particular by James Reason) in order to illustrate particular ways of thinking about culture in relation to safety and incidents[6].

To summarise, just culture is hard-wired in a network of heterogeneous elements, ranging from monitoring systems to diagrams and metaphors. Each element is important, but it is their juxtaposition that makes just culture workable. Having either soft elements or monitoring systems only would not provide sufficient leverage, considering the complexity of operations and the variety of organisational roles (e.g., pilots, crew, non-flying members of staff). As put by a senior manager, when prompted to reflect on whether softer elements were superfluous in the presence of pervasive monitoring systems, "I like to picture it as the image on the US dollar bill, you have the all seeing eye at the top of the pyramid looking into the organisation, more a case of big 'brothers' watching you, the eye (soft elements) and flight data monitoring (technology)[7]."

Interacting via technology

A second characterising element that emerges from *Airline*'s safety practices relates to the interactive control style that they promote. Control technologies of *Airline* are designed to

of a safety management system without a full understanding of how these components add up to form a safe working environment.

[6] For example, it was possible to observe the use of the production vs. protection diagram, which shows how the degree of protective measures must match the hazards of the productive operations; and the use of the so-called Swiss Cheese model, which shows how risks can be mitigated by multiple types of defenses which are 'layered' behind each other (see Reason, 1997).

[7] Email communication – November 2014.

encourage interactions. This emphasis starts from the very broad approach taken to encourage the reporting of events by not imposing a materiality threshold. As put by a senior safety manager:

> "Well the risk is as soon as you start trying to define what people should report and should not report they won't bother. So you're best to get them to report everything and then get clever how you sort out the chaff from the wheat … So we just say you know, just report everything."

SR's investigators suggested an increasing willingness to engage with the system, and certainly an increase in the usage of the system in the last 6 months. The firm that designed the system stated that *Airline* witnessed an increase by more than 50% in incident reporting within a very short time of SR being deployed. As put by a senior manager, a crucial aspect of their job is "to make it really easy for [employees] to report." For this reason, staff can log into the SR system from almost anywhere[8]. Moreover, once a report is filed in the system, the SR application is designed to make it easier for investigators to ask their peers and experts to comment on or review their investigations and subsequently provide tailored feedback to the reporter.

But the interactive nature of safety work in *Airline* is not of interest simply because people are encouraged to report as much as possible. The *technoculture* of such interactive style can be related to three specific features. First, the reporting technologies encourage an expanded view of the issues being reported, encompassing all sorts of seemingly minor

[8] At the time of the second field visit in May 2014, the company was testing an app that will allow access to the system from people's personal devices.

things and maintaining open for investigation a multiplicity of risk objects (Hilgartner, 1992). As put by a senior manager:

> "So the safety reports tell us what the reporter observed or thought happened and might get a bit about why they thought it happened and we try and verify that through the investigation process. Flight data monitoring will tell you exactly what the aeroplane did but not why. Electronic training reports will tell you how a large group of people are likely to behave in a given non-normal situation. This will tell you about the reliability of equipment and there's a whole bunch of other stuff here, on-time performance, fuel, all components of that picture."

The initial piece of information travels from the actual place of an incident and is placed into a network of relations between elements that come from many other places, from distant materials and faraway actors. A wide range of objects, besides senior managers and subordinates, safety and non-safety people, contribute to make control technologies interactive, stimulating reflections and raising further questions on a specific incident case. These elements not only contribute to form a more comprehensive view of what and why something happened. But they are also potentially transformed as part of an emerging socio-technical network around a specific safety issue (Hilgartner, 1992). Drawing on the previous quote, electronic training reports help to explain flight data monitoring information, which in turn add context to the reporter's perceptions of an event.

Second, the technology is designed to expand functionalities and working interactions. The technology is a vehicle for different types of touch points that occur between safety personnel and the rest of the organisation. But the nature of these interactions, though varied, has a specific common logic. SR is a forensic system, where everything done can be traced and where audit trails are preserved (i.e., the investigator can print different forms at different stages of the inquiry). The web-based application allows for the tracking of the report to the point of delivery, and is constantly verifying the robustness of the audit trail generated by each investigation. In so doing, the application is also disciplinary in the sense that it controls the workflow timings, for example with notifications on late responses approaching deadlines (although it also allows due dates to be re-set as needed and request date extensions).

Third, interactions are frequent and mediated by reporting technology. This observation provides a counterpoint to previous research on management control systems and safety experts' work. Well-known research on interactively-used control systems (e.g., Simons, 1995) emphasises the importance of the big 'strategic' uncertainties that require face-to-face time in regular meetings between senior managers and subordinates. Interviews and direct observation at *Airline* show instead frequent interactions, which are mediated by the reporting technologies and are sustained by a relentless interest in small, and possibly trivial, things and massive archiving systems. Moreover, prior work on safety in the airline industry (e.g., Macrae, 2007a, 2007b) emphasises the relevance of participative networks to cope with the perceived incompleteness of incident reporting data; investigators act as 'coordinating hubs' by informing others about signs of potential risks, requesting reviews

and other information from specialists, and also forming temporary and distributed teams of experts. In *Airline*, the reporting technology seems to operate as a key 'coordinating hub', with a great deal of interaction which is not face-to-face, but enabled and mediated by technologies such as the SR system.

To summarise, just culture is hard-wired in a network of heterogeneous elements, which is a vehicle for different types of touch points and an expanded view of the issue being reported initially. Interaction is encouraged (i.e., easy access to reporting technology, absence of a materiality threshold), but mediated by reporting and monitoring technologies that contribute to control workflow timings and preserve an audit trail of what is being done. In such context, what is the role of safety experts? This question will be addressed in the next section.

Business partnering

The way in which organisational actors answer questions related to the area of responsibility of functional experts (risk managers in particular), and their position within the organisation structure, has cultural implications, reflecting different values, norms and assumptions around the way in which an organisation sees and acts on risks (Power et al., 2013). Prior literature has explored the changing role of the risk manager in organisations (see Power, 2007; Mikes, 2009, 2011; Hall et al., 2015). On the one hand, risk managers can be technical experts of a sub-discipline of risk management (e.g., financial, safety, information technology risks). On the other hand, especially with the rise of a holistic

conception of risk and risk management, risk managers can be seen as change facilitators and business partners. In the latter case, what matters are relational skills rather than 'technical' and abstract bodies of risk management knowledge.

In fact, the way in which such a business partnering role is exercised by functional experts such as risk managers is a phenomenon that awaits further research and critical assessment (see Mikes in this volume). In *Airline*, the hard-wiring of culture in control technologies and the expansion of working interactions via technology are interrelated with one aspect of business partnering: the ambition to build up respect for safety people and technologies. This ambition can be traced in two interrelated characteristics of the way in which personnel of the Safety Department work.

First, the personal background of safety staff is strongly related to the company's operations. There was a need to add what was called "content and background" to analyse the safety data and to participate in business decisions. Business knowledge was a precondition for interaction with front-line and other staff functions in order to: understand which language to adopt for enhancing authority and credibility; become trusted business advisers; understand the outputs of reporting technologies. A range of informal techniques were used by the Safety Department in order to build respect and trust. Many of these involved facilitating peer-to-peer communication capability and providing a safe environment for people to act naturally and 'speak up' if there are problems. An example is provided in the following quote:

> "We do things such as line orientated safety audits and we put a trained person on the jump seat of the aircraft, he's not a training captain, he's not a manager, he's just one of their colleagues but we train him in observation. And they observe the flights against a threat in aero-taxonomy and we get a huge amount of information from that because what we're trying to do is observe the most natural behaviour we can of that pilot. As soon as we put a manager in there or a training captain, you're going to get their best behaviour. *You put their mate in there and you're more likely to get the nearest you can to what's happening day in, day out*." (Emphasis added)

Second, safety personnel developed success stories about occasions where decisions supported by the Safety Department added value to the company. The precautionary logic of safety (e.g., to avoid people getting hurt) is intertwined with narratives of value creation and 'win-win' situations in terms of safety, costs and business development. Stories of value creation are also based on the development of monitoring and reporting technologies. The design and implementation of the SR system is itself framed as a profitable investment for the company, besides the obvious benefits related to data collection and analysis. Instead of buying a product on the market, the decision was made to build the technology in partnership with a company working on mobile and web-based safety and compliance services. As put by one senior manager:

> "So we decided what we had to do is to build our own system and so then we went back out to the market and said 'We want to build this system, who can help us?' And we found one company that said 'Oh yeah, we get it' and bothered to listen, a company called [name omitted] and so basically we entered a partnership with them whereby we provide the intellectual property around the design and they build the system. They then go off and sell the system to everybody and we get some of the royalties back."

This decision, according to senior managers, was characterised by "lots of wins." Besides benefits in terms of cost and design customisation, supplier risk was also decreased and discounts were obtained from an insurance perspective since, as put by one senior manager, "you're continuing to demonstrate risk management and giving them confidence."

Technoculture and riskwork

As suggested in the introduction to this volume, the motif of riskwork encourages a focus on situationally-specific forms of work. In line with this perspective, in this section I sketch two vignettes that aim to capture just culture in practice and the deeply intertwined relationship between culture and control technology. The vignettes provide short descriptions of situations (e.g., landing airplanes, opening doors,) in which safety data were used to change current practices and behaviour. In line with the riskwork emphasis on

work and 'normal' operations in risk management (see Power in this volume; Bourrier, 2002), the focus is on how members of *Airline* worked to change their and their colleagues' visions and cognitive maps in order to improve daily situations.

On landing airplanes

> Flight data monitoring data show landings outside the normal parameters. Is that risky? This really depends on the airport where the airplane has landed. The data shows that it's happening primarily in the summer in very long runways. It is likely that people are doing visual approaches as opposed to longwinded instrument approaches. There can be economical benefits and positive performance effects (e.g., reduced transfer time to the terminal buildings). There is no immediate risk. But there is a latent risk that people get used to that behaviour. And, after a number of long landings, the model for a long runway may be unconsciously applied to a short runway. That is a problem. Behaviour has to be modified. Flight monitoring data people were taking photographs of Google satellite images and were overlaying on top of that the actual touchdown point on the runway where the aircraft was, and then sending this directly to the crew, saying: "how do you feel about it?"

This vignette reveals elements of the three features of *technoculture* sketched in the previous sections. First, the safety control and reporting technologies contribute to identifying the issue even in the absence of self-reporting. This is important as in complex

organizations such as airlines risks are rarely self-evident (Macrae, 2007a). In fact, under certain conditions, a long landing may not be seen as a problem; on the contrary, it may have some beneficial consequences. As shown in the vignette, the risk materializes only under certain conditions (e.g., a short runway!). Yet there is a latent risk that the 'long landing' approach becomes the norm, and therefore is applied in the wrong context. As put by one interviewee, "ideally what you want to do is, as that risk starts to emerge in the corner, you want to be able to go and address it before it materialises into something uncomfortable."

Second, the vignette shows how an incident investigation is constituted by a number of different elements that come from many different places. Interactions are premised on capturing as much data as possible to extract patterns, trending and correlations and understand what may become a norm, constituting a threat to flight safety. As put by one interviewee, the key aspect is the "process of bringing context in all the time", by using data and interacting with front-line people and other functional experts. The reporting or identification of a long landing is only one component of a much larger information set that informs interactions between safety people and their colleagues. Triangulating different sources of data and analyzing trends helps to understand where long landings are happening and to formulate assumptions about the underlying rationales (e.g., good weather, panoramic approaches to landing, fuel savings, etc.). Although there is an audit trail of the evidence being analyzed, the investigation is not necessarily punitive, but aims to understand behaviour that may incorporate latent risks. Data-supported interaction helps

to make clear why an issue such as long landing is important and needs to be addressed even if, in the first instance, it is not perceived as a risk.

Third, corrective actions suggest a business partnering approach that emphasise "mate-to-mate" conversations with the help of visual aids. Senior managers acknowledge that it would be easy to put a safety note out recommending to avoid bad behaviour. But the same message can be conveyed with "a sense of humor" not to shame people but making it obvious that there is something wrong with long landings. As put by one interviewee: "It's not bossy, it's facilitative thinking you know, you're helping … you're taking people with you on a journey, this is the preferred modus operandi."

In addition to communication methods and 'attention-grabbers' such as the above, the Safety Department relies on a network of liaison officers. Their goal is to facilitate peer-to-peer communication and increase the number and quality of touch points between safety and the front-line personnel. One senior manager said that "their job is to … give people feedback as peer-to-peer, in confidence, to improve performance." Interestingly, similar to technologies of control such as flight data monitoring, liaison officers can be seen as a means to penetrate the daily working practices of crew members. But they are also a way to enhance confidence and trust in safety workers: in short, to build respect for the Safety Department.

On opening doors

> The doors of an aircraft have automatic escape slides so that if you open them in an emergency the slide automatically inflates. These automatic slides need to be disarmed when embarking passengers normally. If this is not done, there is a safety risk because if someone is standing on the steps and one of these slides explodes, it can hit the person with harmful consequences. A specialist was asked to break down the current task (the opening of the door under normal conditions) and understand why the safety risk may occur. The specialist and his support team designed a new task. The investment in having that specialist in to work on the task design was about £10,000. But every time the problem had occurred in the past, the company had to throw away the slide and buy a new one.

The safety risk illustrated in the vignette is perhaps more evident than the preceding one. If a problem occurs, then it is likely that someone has been injured and, at least, a material loss has happened. In line with the chapter's motif of *technoculture*, this vignette shows how the reporting of safety events is only the starting point for a learning process which is premised on a relentless interest in data collection and analysis.

The reporting system showed that this problem had been occurring at *Airline*, although at a lower rate compared to the industry average. In this specific case, available data suggested a cyclical pattern. The occurrence of the problem decreased following a change in the procedure, but then tended to rise again for various reasons such as the intake of new hires. As in the previous vignette, the collection of data on the single 'fact' (problems with the opening of a door on flight X at airport Y on date Z) coexists with an aspiration to

understand its underlying causes. Different sources of information are juxtaposed (e.g., incident reporting, new hires); interactions with colleagues from different functions take place, and external specialists are consulted.

The disciplinary element of technology (e.g., "has someone made a willful mistake?") is only one part of the story. Learning from the data is also crucial. In fact, the remedial actions are informed by a recognition of human fallibility. The company draws on a "hierarchy of effectiveness" of safety measures, which ranges from redesigning a component (e.g., the door) to increasing awareness via communication campaigns. The benefits, costs and uncertainty of alternative measures are taken into consideration: for instance, the redesign of a door is a massive cost, has large potential benefits, but also uncertainty as the problem may occur even with the redesigned door. As put by an interviewee: "So right at the top is the design … Right at the bottom is a notice to crew to say 'Don't forget to check you've disarmed the doors before opening them' and that's almost useless."

Compared to the previous case, this vignette specifically illustrates the way in which an issue gets traction and is acted upon. Two elements emerge. The first involves a risk-based rationale. The company has hundreds of flights in a day, and the four doors of the airplane are opened twice per flight. Being a very routine job, even in the context of very low probability for the event to occur, the exposure is significant. The second element is related to the way in which safety experts can expand their organisational footprint. A general problem for functional experts such as risk managers is to justify the value of their recommendations (see Power, 2007; Power et al., 2013; Hall et al., 2015). The vignette

suggests an explicit cost-benefit analysis related to the intervention recommended by the Safety Department. As put by one interviewee:

> "And the investment we made in having that person in to help us was probably about £10,000 but every time we blow a slide we have to throw it away and buy a new one. So we will have reaped the safety benefit and the direct cost and had less on-time performance impacts as a consequence because we're not having to wait for a new slide to be shipped in. So it's a win-win all round."

On this basis, this vignette reinforces the view that the partnering role of safety experts is not only based on relational skills, 'attention-grabbers', and liaison figures. It is also about developing a narrative of value-effectiveness through straightforward success stories. As put by one interviewee:

> "And if you're thinking about you know, the upside of that in terms of the business, *well my example absolutely demonstrates the safety benefit, the direct cost benefit, the operational efficiency benefit* and that's what we're trying to do in this big programme. But it all fits in with this concept of a safety culture and learning culture and supporting culture and nurturing culture you know, just culture." (Emphasis added)

Concluding reflections

In this chapter, I explored how technology and culture are co-produced and characterize specific kinds of riskwork in the aviation sector, namely efforts to promote 'speaking up' via risk reporting systems and subsequent analysis. The material collected from the Safety Department of a large airline company draws attention to the way in which a narrative is developed around the concept of just culture and how such narrative is intertwined with control technologies.

The co-production of technology and culture is captured through the motif of *technoculture*, which expresses three themes: the hard-wiring of just culture into control technologies; the technology-supported expansion of working interactions; and business partnering to build respect for safety values, people and technologies. Two vignettes related to routine events, such as landing airplanes and opening doors, add color to the features of riskwork as *technoculture.* Specifically, we see the "no corners to hide" dimension of just culture, but also its aspiration for a learning culture supported by granular data collection and analysis; we see the emergence of new, more or less cooperative, interactions across internal functions but also with external actors; we also see the development of narratives that reinforce the value-added role of the Safety Department, as well as 'attention-grabbers' and new communication lines in action.

This chapter started with a set of questions that stressed how risk reporting and analysis are riddled with ambiguities and contradictions: risks are not self-evident; reporters as well as the receivers of information are biased and fallible; there is an inherent tension between the need for risk accountability, financial and legal liability for risk, and the ambition to encourage risk reporting and 'speaking up.' Drawing on the *technoculture* concept, this

chapter suggests that these tensions are addressed in practice by dynamic networks of heterogeneous elements, which stimulate and mediate interactions among safety and non-safety experts. Such socio-technical networks give expression to, rather than suppressing, the ambiguities inherent in risk reporting and analysis. There is an encouragement to report that is not blame-less; there is help and support from safety personnel, but also pervasive monitoring via systems and local networks of liaison officers; there is a focus on flying staff, but also recognition of other members of the organisation and their potentially relevant role in just culture. Recent uses of the concept of organisational (risk) culture as 'the way we do things around here' stress shared understandings and solutions to common problems that can be engineered to achieve optimal solutions (see Power et al., 2013). On the contrary, *technoculture* recognizes, and even nurtures, the plurality of values and commitments that characterise riskwork.

In closing, it is appropriate to make a comment on the process of writing about organisational culture. Text about organisational culture like this chapter should be read in the context of the author's situation at the moment in which the text is developed (Kunda, 1992: Ch. 6; Smircich, 1995; Yanow, 1995). Accordingly it is important to understand that *Airline* was initially conceived as a comparator case in the context of a broader research project on risk culture in financial organisations (see Power et al., 2013). The aim was to obtain a point of contrast that could stimulate new questions and lines of thought. This specific circumstance influenced the shape this chapter and the development of *technoculture* as an organising concept. If the idea of *technoculture* plausibly describes features of practice in the aviation industry, it also provides many points of contrast with

the financial sector. Examples of such points of contrast were: the lack of emphasis in *Airline* on formalised models that articulate different responsibilities over risk oversight and management; the remarkable degree of openness to the external world and respect for external advisers (including academic experts!); the lack of concerns about any dilution or capture risks (i.e., 'going native' problem); awareness that "context is crucial" and the need for having time to reflect as much as to collect and analyse quantitative data.

So the appeal of *technoculture* in this chapter is shaped by the points of contrast with financial services organisations as much as by the data collected from *Airline* itself. There are certainly limitations to such an approach such as a limited understanding of field level practices in the aviation industry. However, data from *Airline*, and related reflections, helps to transform culture from a "tired answer" into an "interesting question" (Smircich, 1995: 235). This is priceless for researchers confronted with an ever expanding production of texts that point to culture as a black-box explanation of last resort, both for the financial crisis and other spectacular failures.

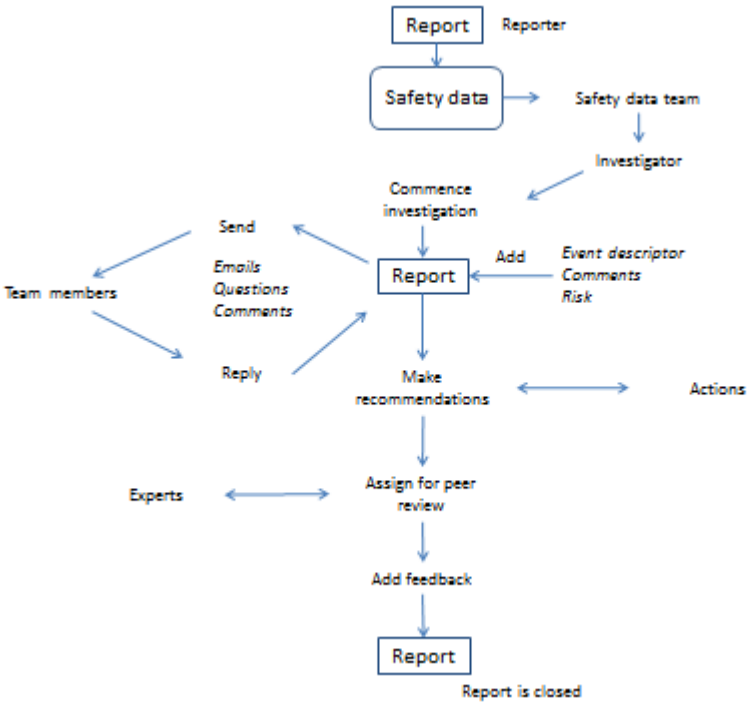

Figure 7.1: Safety reporting system at *Airline*

References

AIRMIC, ALARM, & IRM. (2002). *A Risk Management Standard*, pp. 1–17. Retrieved from: <www.theirm.org/knowledge-and-resources/risk-management-standards/irms-risk-management-standard/>

Alvesson, M. (2002). *Understanding Organizational Culture*. London: SAGE Publications.

Barley, S. R., & Kunda, G. (2001). Bringing Work Back In. *Organization Science*, 12(1), 76–95.

Bijker, W.E., Hughes, T. P., & Pinch, T. (Eds). (1987). *The Social Construction of Technological Systems*. Cambridge, MA: MIT Press.

Bourrier, M. (2002). Bridging Research and Practice: The Challenge of "Normal Operations" Studies. *Journal of Contingencies and Crisis Management*, 10(4): 173–80.

Callon, M. (1987). Society in the Making: The Study of Technology as a Tool for Sociological Analysis. In Bijker W.E., Hughes T. P., & Pynch T. (Eds), *The Social Construction of Technological Systems* (pp. 83–103). MIT Press: Cambridge, MA.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004). *Enterprise Risk Management — Integrated Framework. Executive summary*, pp. 1–

16. Committee of Sponsoring Organizations of the Treadway Commission. Retrieved from <www.coso.org/documents/coso_erm_executivesummary.pdf>

Hall, M., Mikes, A., & Millo, Y. (2015). How Do Risk Managers Become Influential? A Field Study of Toolmaking in Two Financial Institutions. *Management Accounting Research*, 26/1: 1–20.

Hilgartner, S. (1992). The Social Construction of Risk Objects: Or, How to Pry Open Networks of Risk. In Short J.F. & Clarke, L. (Eds), *Organizations, Uncertainties and Risk* (pp. 39-53). Boulder, CO: Westview Press.

International Standards Organisation (ISO). (2009). *ISO 31000:2009 - Risk Management Principles and Guidelines*. Retrieved from <www.iso.org/iso/home/standards/iso31000.htm>

Kaplan, R., & Mikes, A. (2012). Managing Risks: A New Framework. *Harvard Business Review*, June, 49–60.

Kunda, G. (1992). *Engineering Culture: Control and Commitment in a High-Tech Corporation*. Philadelphia, PA: Temple University Press.

Macrae, C. (2007a). *Interrogating the Unknown: Risk Analysis and Sensemaking in Airline Safety Oversight*, pp. 1–18. London: Centre for Analysis of Risk and Regulation (CARR). Retrieved from <http://www.lse.ac.uk/accounting/CARR/publications/discussionPapers.aspx>

——. (2007b). *Analyzing Near-miss Events: Risk management in Incident Reporting and Investigation Systems*, pp. 1–24. London: Centre for Analysis of Risk and Regulation (CARR). Retrieved from <http://www.lse.ac.uk/accounting/CARR/publications/discussionPapers.aspx>

Mikes, A. (2009). Risk Management and Calculative Cultures. *Management Accounting Research*, 20(1), 18–40.

——. (2011). From Counting Risk to Making Risk Count: Boundary-work in Risk Management. *Accounting, Organizations and Society*, 36 (4-5), 226–45.

Power, M. K. (2007). *Organized Uncertainty: Designing a World of Risk Management*. Oxford: Oxford University Press.

Power, M. K., Ashby, S., & Palermo, T. (2013). *Risk Culture in Financial Organisations - A Research Report*, pp. 1–103. London: Centre for Analysis of Risk and Regulation (CARR). Retrieved from <www.lse.ac.uk/researchAndExpertise/units/CARR/pdf/Final-Risk-Culture-Report.pdf>

Reason, J. T. (1997). *Managing the Risks of Organizational Accidents*. Aldershot, Hants: Ashgate.

Schein, E. H. (2004). *Organizational Culture and Leadership*, 3rd ed. San Francisco, CA: John Wiley & Sons, Inc.

Simons, R. (1995). Control in an Age of Empowerment. *Harvard Business Review*, March-April, 80–8.

——. (1999). How Risky is Your Company? *Harvard Business Review*, May-June, 85–94.

Smircich, L. (1995). Writing Organizational Tales: Reflections on Three Books on Organizational Culture. *Organization Science*, 6 (2), 232–7.

Vaughan, D. (1996). *The Challenger Launch Decision: Risky Technology, Culture and Deviance at NASA*. Chicago: University of Chicago Press.

Weick, K. E., & Sutcliffe, K. M. (2007). *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*, 2nd ed. San Francisco: Jossey-Bass.

Yanow, D. (1995). Writing Organizational Tales: Four Authors and Their Stories about Culture. *Organization Science*, 6 (2), 225–38.